Nota van Inlichtingen 2: 'SIEM SOC'

Referentie: IBMN-2026-VIJ-CM-001

Gemeente Vijfheerenlanden

Datum : vrijdag 30 oktober 2026

Vraag	Verwijzing	Vraag	Antwoord Martin
1	Aanbestedingsdocument SIEM SOC	Referenties – type organisatie. In §3.2.1 wordt voor Kerncompetentie 1 en Kerncompetentie 2 (punt 1) ervaring gevraagd bij 'een gemeentelijke organisatie' met een hybride ICT-infrastructuur van tenminste 420 gebruikers. Vraag: Kan de aanbestedende dienst bevestigen dat ook referenties bij andere overheidsorganisaties (zoals rijksdiensten, uitvoeringsorganisaties, provincies, waterschappen en (semi-)publieke kennisinstituten) worden geaccepteerd, mits deze qua omvang (tenminste 420 gebruikers) en complexiteit (hybride ICT-infrastructuur, on-premises én Cloud) gelijkwaardig zijn aan een gemeentelijke organisatie?	Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie.
2	Aanbestedingsdocument SIEM SOC	Referenties – kleinere organisatie of kleine overheidsdienst als alternatief. §3.2.1 vraagt voor beide kerncompetenties ervaring bij een gemeentelijke organisatie met een hybride ICT-infrastructuur van tenminste 420 gebruikers. Wordt een referentie bij een (iets) kleinere gemeentelijke organisatie met minder dan 420 gebruikers geaccepteerd, indien de ICT-omgeving qua complexiteit gelijkwaardig is (hybride infrastructuur, aantal en soort aangesloten logbronnen, 24x7 SOC-dienstverlening)? Zo ja, wat is de ondergrens in aantal gebruikers?	"Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie met tenminste 420 gebruikers. De gemeente Vijfheerenlanden is een organisatie met ongeveer 700 gebruikers. De 420 gebruikers (60% van het totaal) is daarmee de ondergrens van gebruikers."
3	Bijlage A1 – Programma van Eisen non-functionals	ISO 20000 – moment van beschikken en gelijkwaardigheid. Eis TECH13 luidt: 'De Opdrachtnemer beschikt over een ISO20000 IT servicemanagement certificaat of vergelijkbaar. Indien vergelijkbaar toelichting op de procedures.' Op welk moment moet het ISO 20000-certificaat (of het vergelijkbare certificaat) aanwezig zijn: op de inschrijfdatum, bij het voornemen tot gunning of de ondertekening van de overeenkomst, op de ingangsdatum van de overeenkomst (1 maart 2027), of binnen een nader te bepalen termijn daarna? Is het acceptabel dat een inschrijver op de inschrijfdatum nog in het certificeringstraject zit (audit loopt of is gepland, certificaat nog niet afgegeven), bijvoorbeeld met bewijs van de auditplanning en een toezegging het certificaat uiterlijk op de door de aanbestedende dienst te bepalen datum te overleggen? Wat beschouwt de aanbestedende dienst als 'vergelijkbaar' certificaat of gelijkwaardige borging (bijvoorbeeld een ander erkend certificaat voor IT-servicemanagement, of ISO/IEC 27001 in combinatie met aantoonbaar ingerichte ITSM-processen), en welke 'toelichting op de procedures' wordt dan verwacht?	"Op dinsdag 20 oktober 2026 jl. is middels een mededeling van aanbestedende dienst in een 1e Nota van Inlichtingen het volgende medegedeeld: 'De aanbestedende dienst deelt u hierbij mede dat in het document 'Bijlage A1 - Programma van Eisen – non functionals dd 08-10-2026' per abuis een uitvoeringseis is blijven staan die niet van toepassing is op deze aanbesteding. Het betreft de eis: ""De Opdrachtnemer beschikt over een ISO20000 IT servicemanagement certificaat of vergelijkbaar. Indien vergelijkbaar toelichting op de procedures.' Deze eis vervalt!' Uw vraag is derhalve niet meer van toepassing."

4	Bijlage A1 – Programma van Eisen non-functionals	Boeteclausule SLA26 en concept-SLA. SLA26 koppelt de boete aan het aantal incidenten per maand (Prio 1: twee of meer = 100% van de maandelijkse kosten; Prio 2: 50%; Prio 3 en 4: 25%), terwijl SLA 1.2 spreekt van sancties 'bij niet-naleving door opdrachtnemer' en SLA8 detectietijd, reactietijd en escalatietijd als doorlooptijden benoemt. Bedoelt de aanbestedende dienst een boete bij het niet halen van de overeen te komen doorlooptijden per prioriteit, of een boete bij het optreden van beveiligingsincidenten zelf, ook indien deze tijdig zijn gedetecteerd en afgehandeld?	De boeteclausule is bedoeld als sanctie op het niet naleven door de opdrachtnemer van de overeengekomen servicenormen en verplichtingen, waaronder de toepasselijke detectie-, reactie-, meld- en escalatietermijnen en de overige SLA-afspraken. Het enkele optreden of aantal beveiligingsincidenten vormt op zichzelf geen grond voor een boete, indien de opdrachtnemer deze incidenten overeenkomstig de afgesproken normen detecteert, classificeert, meldt en opvolgt. De boete wordt dus gekoppeld aan tekortkomingen in de dienstverlening van de opdrachtnemer, niet aan het bestaan van beveiligingsincidenten als zodanig.
5	Aanbestedingsdocument SIEM SOC	Social return – grondslag, opties, spreiding en invulling. §6.6 legt een social return verplichting op van 2% van de opdrachtwaarde. Bijlage J (Bijlage A, definitie 16) definieert de opdrachtwaarde als 'de totale waarde van de opdracht, exclusief btw, inclusief eventuele opties of verlengingen van de overeenkomst'. Bevestigt de aanbestedende dienst dat de grondslag de totaalprijs op het inschrijfbiljet is (maximale looptijd van 9 jaar, exclusief btw)? Opdrachtnemer is gevestigd buiten de AV regio, accepteert opdrachtnemer een SROI invulling in de regio van opdrachtnemer conform de gestelde kaders in het document?	Wij gaan er vanuit dat uw conclusie correct is. Echter pas na gunning van de opdracht zal de winnende partij afstemming hebben met het Adviespunt Social Return over de daadwerkelijke wijze van invulling van Social Return. Naar verwachting is deze inderdaad gebaseerd op de totale waarde van de opdracht, exclusief btw, inclusief eventuele opties of verlengingen van de overeenkomst (en dus 9 jaar).
6	PVE 2.23	In de eis spreekt de opdrachtgeven over de eigendom van "gegevens, use-cases, klant specifieke detectieregels, rapportagesjablonen, connectorconfiguraties, playbooks, workbooks, dashboards en overige klant specifieke configuraties". Wat bedoeld de opdrachtgever in deze context met use-cases?	Met use-cases bedoelt de opdrachtgever de afgesproken, concrete detectiescenario's voor het signaleren van beveiligingsdreigingen en afwijkende activiteiten binnen de gemeentelijke omgeving. Een use-case beschrijft bijvoorbeeld welk gedrag of welke combinatie van signalen wordt onderzocht, uit welke logbronnen de benodigde gegevens komen en welke detectieregels, correlaties of andere logica worden gebruikt om een melding of incident te genereren. De use-cases omvatten daarmee, mogelijk naast de generieke use-caes van Opdrachtnemer, klantspecifieke uitwerking en inrichting in de SIEM/SOC-omgeving, waaronder de bijbehorende detectielogica en configuratie. Dit sluit aan bij de in het Programma van Eisen genoemde initiële use-cases en de eisen voor het gezamenlijk opstellen, testen, autoriseren, documenteren en onderhouden van klantspecifieke detecties.
7	PVE 6.3 & 7.2	In 2.23 staat dat de opdrachtgever eigenaar is en blijft van klant specifieke detectieregels. In 6.3 en 7.2 staat dat de opdrachtgever eigenaar is en blijft van alle detectieregels. Kan de opdrachtgever bevestigen dat alleen klant specifieke detectieregels eigendom is en blijft van de opdrachtgever?	De opdrachtgever bevestigt dat de eigendomsbepaling ziet op de klantspecifieke detectieregels die binnen de opdracht voor de gemeente worden ontwikkeld, ingericht of aangepast. Reeds bestaande generieke detectieregels en generieke intellectuele eigendomsrechten van de opdrachtnemer worden hierdoor niet eigendom van de opdrachtgever. De opdrachtgever krijgt voor die generieke onderdelen wel de gebruiksrechten die volgens de aanbestedingsstukken nodig zijn voor de uitvoering, continuïteit en overdracht van de dienstverlening. De formulering "alle detectieregels" in eisen 6.3 en 7.2 moet in samenhang hiermee worden gelezen en ziet op de detectieregels die specifiek voor de opdrachtgever zijn ontwikkeld of ingericht.
8	DAP	Mag de aanbieder net zoals bij de SLA een voorbeeld DAP meesturen inclusief RACI's overzicht. Deze zal als startmodel gebruikt worden om na gunning de DAP verder te specifiëren.	Ja, de aanbieder mag bij de inschrijving een voorbeeld-DAP meesturen, inclusief een RACI-overzicht. Dit voorbeeld geldt uitsluitend als startmodel. Na gunning wordt het DAP door opdrachtgever en opdrachtnemer gezamenlijk verder uitgewerkt en afgestemd op de daadwerkelijke inrichting, dienstverlening en verantwoordelijkheidsverdeling. Het DAP en de RACI-matrix worden vóór ingebruikname vastgesteld, overeenkomstig de eisen in het Programma van Eisen.

9	Documenten	In de aanbesteding beschrijft de opdrachtgever dat de maximale uitwerking van de subgunningscriterium A, B en C 8 pagina's is. Zijn dit 8 inhoudelijke pagina's en dus exclusief voorblad, bijlages, inhoudsopgaves etc.?	Ja dit zijn inderdaad 8 inhoudelijke pagina's en het is dus akkoord dat dit exclusief voorblad, inhoudsopgave en eventuele bijlage(s) is. Als bijlagen buiten de acht inhoudelijke A4 mogen uitsluitend de planning en het RACI-model worden toegevoegd.
10	Prijzenblad	Kan de opdrachtgever nader specificeren wat precies bedoeld wordt met Honeypots/Deceptietechnologie? Een volledige honeypot (server) inrichten met logstreams en detecties is natuurlijk veel meer werk dan een simpele honeytoken (nep account of bestand) plaatsen in het netwerk.	Met honeypots/deceptietechnologie bedoelt de opdrachtgever het inzetten van misleidende, niet-productieve digitale objecten of voorzieningen om ongeautoriseerde activiteiten vroegtijdig te signaleren. Dit kan bijvoorbeeld een beperkte honeypotdienst of -systeem zijn, maar ook een honeytoken, zoals een nepaccount, een fictief bestand of een andere lokvoorziening. De opdrachtgever verduidelijkt dat met Honeypots/Deceptietechnologie drie typen voorzieningen kunnen worden aangeboden: **Honeytoken:** een misleidend digitaal object zonder eigen dienst of systeem, geplaatst in de bestaande omgeving. Voorbeelden zijn een fictief (beheer)account in Active Directory of Entra ID, een nepbestand, fictieve credentials, een API-sleutel of een DNS- of URL-token. Elke poging om het object te benaderen of te gebruiken genereert een melding aan de SIEM/SOC-omgeving. **Low-interaction honeypot:** een lokvoorziening die één of meer netwerkdiensten nabootst, bijvoorbeeld RDP, SMB, SSH of een webinterface, zonder een volledig werkend besturingssysteem aan te bieden. De aanvaller kan beperkt interacteren. De honeypot registreert verbindingspogingen, scans en inlogpogingen en stuurt hierover meldingen naar de SIEM/SOC-omgeving. Het risico op misbruik van de voorziening zelf is laag. **High-interaction honeypot:** een volwaardige, afzonderlijke lokserver of vergelijkbare omgeving met een echt besturingssysteem en echte diensten, die zich voor een aanvaller gedraagt als een productiesysteem. De aanvaller kan uitgebreid interacteren. Zo krijgt de opdrachtgever inzicht in werkwijze, gebruikte tooling en beoogde laterale beweging. Deze variant omvat ook de bijbehorende logging, specifieke detecties, isolatie ten opzichte van de productieomgeving en SOC-opvolging. Inschrijvers nemen in het gewijzigde prijzenblad, dat als bijlage 1 aan deze Nota van Inlichtingen is toegevoegd, voor elk van deze drie typen een afzonderlijke vaste prijs op.
11	Prijzenblad	De kolom “Aantal” in het prijzenblad is leeg. Daardoor rekent elke inschrijver met eigen aannames en zijn de totaalprijzen niet te vergelijken. Wilt de opdrachtgever per logbron de eenheid en het aantal invullen in een aangepast prijzenblad? Wij stellen voor: in elk geval aan het aantal actieve gebruikers (zonder serviceaccounts), werkstations, servers en netwerk appliances (Cisco Meraki, Barracuda, SecureMe2).	Voor de post Honeypots/Deceptietechnologie verwijst de opdrachtgever naar het antwoord op vraag 10 in deze Nota van Inlichtingen.
12	prijzenblad	Verwacht de opdrachtgever dat de opdrachtnemer ook detectieregels ontwikkeld voor de prijs die aangegeven wordt per logbron zoals HelloID, DHCP, DNS? Dit wordt zo wel gesuggereerd in PVE5.5. Hoeveel detectieregels zijn dan inclusief aan de prijs die de aanbieder moet opgeven?	Ja. De prijs per logbron in het prijzenblad omvat de werkzaamheden die nodig zijn om de betreffende logbron aan te sluiten en de overeengekomen dienstverlening daarvoor uit te voeren. Dit omvat ook het toepassen en onderhouden van passende standaarddetecties die bij de logbron en de aangeboden SIEM/SOC-dienstverlening horen. De aanbestedingsstukken schrijven geen vast aantal detectieregels per logbron voor. De inschrijver vermeldt daarom in zijn inschrijving welke standaarddetecties en use-cases voor de genoemde logbronnen beschikbaar zijn en welke daarvan binnen de opgegeven prijs vallen.

13	PVE 5.5	In 5.5 staat dat de prijs voor de logbron ook de dataingestion moet bevatten en de retentie etc. Maar als de gemeente Sentinel in eigen tenant wil behouden (wat we ook aanraden) dan lopen deze kosten rechtstreeks via Microsoft en gaat dat niet via ons als aanbieder. Kan de opdrachtgever het prijzenblad hierop aanpassen?	De opdrachtgever bevestigt dat Microsoft Sentinel binnen de eigen Microsoft-tenant van de opdrachtgever wordt ingericht. Kosten die Microsoft rechtstreeks aan de opdrachtgever in rekening brengt, zoals eventuele kosten voor gegevensinname en retentie, worden daarom niet opgenomen in de prijs per logbron van de inschrijver. De prijs per logbron betreft de kosten voor de werkzaamheden en dienstverlening van de opdrachtnemer, waaronder — voor zover van toepassing — aansluiting en beheer van de logbron en de bijbehorende SOC-dienstverlening. De opdrachtgever past het prijzenblad op dit punt niet aan. Inschrijvers dienen in hun prijsopgave duidelijk onderscheid te maken tussen kosten van Microsoft die rechtstreeks bij de opdrachtgever in rekening worden gebracht en kosten voor de dienstverlening van de opdrachtnemer.
14	prijzenblad	Implementatie maximaal € 15.000 (PvE 5.7). Dat is erg krap voor het opzetten van de gehele setup inclusief 8 logbronnen, de bijbehorende use-cases, HLD/LLD, DAP en opleiding. Is het budgetplafond van € 15.000 een K.O. eis?	HLD en LLD worden losgelaten als eis uit 2.15. De eisen in 2.2 blijven wel van kracht. Onder training wordt verstaan eerder het overdragen en instrueren van stakeholders binnen de gemeente dan dat opleiding suggereert. Dit valt wel verder binnen het eenmalige onboarding budget.
15		De aanvullende advisering voor de uren per jaar wordt niet meegenomen in de totale kosten waarop de aanbieder wordt beoordeeld zoals aangegeven. Maar dat staat haaks op de inhoud van cel H55. Daar staat dat dit wel in de beoordeling zit. Kan de opdrachtgever hier meer uitleg over geven?	Scherp opgemerkt, We hebben de beschrijving in het prijsblad voor H55 aangepast. Deze telt NIET mee voor de beoordeling. Zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.
16	Bijlage E: Document Bewijsstuk Referentie	In Kerncompetentie 1 en 2 wordt ervaring gevraagd bij een gemeentelijke organisatie van tenminste 420 gebruikers. De inrichting en het beheer van Microsoft Sentinel (data connectors, analytics rules, automatisering/playbooks) en de bijbehorende SOC-processen zijn in de basis schaalonafhankelijk. De complexiteit wordt vooral bepaald door de hybride infrastructuur en het aantal gekoppelde bronnen, niet door het aantal gebruikers. Kan de aanbestedende dienst motiveren waarom een ondergrens van 420 gebruikers noodzakelijk is? Is de aanbestedende dienst bereid deze ondergrens te verlagen naar bijvoorbeeld 150 gebruikers, of de eis te formuleren als “een organisatie met een vergelijkbare complexiteit en hybride ICT-infrastructuur”?	Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie met tenminste 420 gebruikers. De gemeente Vijfheerenlanden is een organisatie met ongeveer 700 gebruikers. De 420 gebruikers (60% van het totaal) is daarmee de ondergrens van gebruikers.
17	Bijlage E: Document Bewijsstuk Referentie	Valt onder “gemeentelijke organisatie” ook een gemeenschappelijke regeling waarin gemeenten samenwerken, zoals een veiligheidsregio, een uitvoeringsorganisatie of een regionale belastingsamenwerking? Deze organisaties vallen eveneens onder de BIO en hebben een vergelijkbare ICT-omgeving en vergelijkbare compliance-eisen.	Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie met tenminste 420 gebruikers.

18	Aanbestedingsdocument §3.2.1 (p. 15); Bijlage E	Volgens §3.2.1 toont de inschrijver de kerncompetenties aan “door middel van aparte referentieopdrachten”. Bevestigt de aanbestedende dienst dat de inschrijver voor beide kerncompetenties dezelfde opdracht mag opvoeren, met per kerncompetentie een eigen Bijlage E? Dat geldt dan voor een opdracht die zowel de inrichting en het beheer van Microsoft Sentinel als de 24x7 SOC-dienstverlening omvat. Deze aanbesteding combineert beide onderdelen zelf ook in één opdracht.	De aanbestedende dienst verduidelijkt dat één referentieopdracht voor beide kerncompetenties mag worden gebruikt, mits uit die referentie afzonderlijk en aantoonbaar blijkt dat aan alle eisen van zowel kerncompetentie 1 als kerncompetentie 2 wordt voldaan. De opdrachtgever verlangt dus ervaring met zowel de implementatie en het beheer van Microsoft Sentinel als de 24/7 SOC-dienstverlening, maar eist niet dat deze ervaring uit twee verschillende contracten afkomstig is. De inschrijver moet per kerncompetentie duidelijk maken welk onderdeel van de referentie de betreffende ervaring aantoont. Dit voorkomt dat een passende, geïntegreerde opdracht alleen vanwege de contractvorm buiten beschouwing blijft. De mogelijkheid om één referentie voor meerdere kerncompetenties te gebruiken sluit aan bij het aanbestedingsrechtelijk uitgangspunt dat een referentie meerdere kerncompetenties kan aantonen.
19	Aanbestedingsdocument §3.2.1 (p. 15); Bijlage E	De kerncompetenties vragen ervaring met de “uitvoering én oplevering” van een opdracht in de afgelopen drie jaar. Bevestigt de aanbestedende dienst dat een lopende opdracht voldoet als de inschrijver de inrichting in die periode heeft opgeleverd en het beheer en de SOC-dienstverlening op de inschrijvingsdatum nog uitvoert?	Ja dat is correct.
20	Programma van Eisen eis 2.20 (p. 7) en 4.2 (p. 12); Aanbestedingsdocument §3.2.1, kerncompetentie 2 (p. 15); Bijlage F1, regel “24x7x365 eyes on screen meerprijs t.o.v. piket-dienst”	Het Programma van Eisen vraagt 24/7 triage, analyse en zo nodig escalatie van kritieke en hoge meldingen. Het prijzenblad prijst “24x7x365 eyes on screen” als meerprijs ten opzichte van een piketdienst, en kerncompetentie 2 noemt piketdiensten expliciet. Bevestigt de aanbestedende dienst dat de basisdienst buiten kantoortijden mag bestaan uit continue geautomatiseerde monitoring plus een piketdienst die kritieke en hoge meldingen binnen de SLA-termijnen oppakt? Bevestigt zij ook dat 24x7 eyes on screen een optie zonder afnameverplichting is?	Ja. De aanbestedende dienst bevestigt dat de basisdienst buiten kantoortijden mag bestaan uit uitsluitend geautomatiseerde monitoring met een piketdienst. Op grond van eis 2.20 van het Programma van Eisen moet de SIEM/SOC-dienstverlening 24 uur per dag en 7 dagen per week beveiligingsmeldingen kunnen ontvangen en verwerken. Kritieke en hoge meldingen moeten 24/7 overeenkomstig de overeengekomen termijnen worden getrieerd, geanalyseerd en zo nodig geëscaleerd. De aanbestedingsstukken schrijven niet voor dat dit uitsluitend door permanent aanwezige medewerkers gebeurt; de inzet van automatisering en menselijke analyse is mogelijk, mits aantoonbaar aan de vereiste kwaliteit en termijnen wordt voldaan. De regel ‘24x7x365 eyes on screen meerprijs t.o.v. piket-dienst’ staat in Bijlage F1 onder ‘Scope zonder afnameverplichting’. Deze aanvullende dienstverlening is dus een optie zonder afnameverplichting. De optie doet niet af aan de eisen voor de basisdienstverlening: ook bij een invulling met piketdienst moeten kritieke en hoge meldingen 24/7 binnen de overeengekomen termijnen worden getrieerd, geanalyseerd en zo nodig geëscaleerd.
21	Programma van Eisen eis 4.17 (p. 14) en 6.9 (p. 19); Aanbestedingsdocument §1.1.2 (p. 6)	Geautomatiseerde responsacties, zoals het isoleren van een endpoint of het blokkeren van een account, maken direct ingrijpen mogelijk, ook buiten kantoortijden. Bevestigt de aanbestedende dienst dat de gemeente het mandaat voor zulke acties tijdens de implementatie per use case schriftelijk kan vastleggen, bijvoorbeeld in het DAP? Mag de opdrachtnemer deze acties daarna geautomatiseerd uitvoeren, zonder beoordeling per incident vooraf (eis 6.9)?	Ja. De gemeente kan tijdens de implementatie per use-case schriftelijk vastleggen welke responsacties de opdrachtnemer mag uitvoeren en onder welke voorwaarden. Deze bevoegdheden en mandaten kunnen bijvoorbeeld worden opgenomen in het DAP. Wanneer voor een specifieke responsactie vooraf schriftelijk mandaat is verleend, mag de opdrachtnemer die actie geautomatiseerd uitvoeren zonder dat een medewerker de betreffende analyse of actie vooraf per incident hoeft te beoordelen. Dit volgt uit eis 6.9, die beoordeling door een gekwalificeerde medewerker verlangt, tenzij voor de betreffende actie vooraf schriftelijk mandaat is verleend. Responsacties blijven beperkt tot de vooraf vastgelegde bevoegdheden en mandaten, zoals bedoeld in eis 4.17. De gemeente bepaalt welke acties zij mandateert; zonder zo’n mandaat is voorafgaande beoordeling vereist.

22	Programma van Eisen eis 6.8 (p. 18); GIBIT 2025 art. 13 en 14	Eis 6.8 vraagt voorafgaande schriftelijke toestemming voor AI-functionaliteit die gemeentelijke gegevens verwerkt. Valt de standaard machine-learningfunctionaliteit van Microsoft Sentinel en Defender XDR in de eigen tenant van de gemeente onder deze eis, zoals gedragsanalyse en correlatie? Zo ja, kan de gemeente die toestemming eenmalig geven, bijvoorbeeld in het DAP? Bevestigt de aanbestedende dienst daarnaast dat artikel 13 en 14 GIBIT (algoritmische toepassingen en AI-systemen) niet gelden voor deze standaardfunctionaliteit van Microsoft?	De standaard machine-learningfunctionaliteit van Microsoft Sentinel en Microsoft Defender XDR valt onder eis 6.8, voor zover deze door of op advies van Opdrachtnemer wordt geactiveerd of ingezet. Voorbeelden zijn gedragsanalyse (UEBA), anomaliedetectie en geautomatiseerde correlatie. Hetzelfde geldt voor generatieve AI-functionaliteit, zoals Microsoft Security Copilot, en voor AI-functionaliteit van Opdrachtnemer of derden. Opdrachtgever kan hiervoor eenmalig toestemming geven. Opdrachtnemer legt de beoogde AI-functionaliteit vooraf ter bespreking voor, met de informatie die eis 6.8 voorschrijft: doel, gebruikt model, verwerkte gegevens, gegevenslocaties, betrokken subverwerkers, risico's en menselijke controle. Na bespreking en goedkeuring door Opdrachtgever wordt de toegestane AI-functionaliteit vastgelegd in het DAP. Nieuwe of gewijzigde AI-functionaliteit wordt opnieuw ter bespreking en goedkeuring voorgelegd. Eisen 2.6, 2.27 en 6.2 blijven onverkort van toepassing. Artikelen 13 en 14 GIBIT 2025 gelden niet voor de standaardfunctionaliteit van Microsoft die Opdrachtgever rechtstreeks bij Microsoft afneemt. Deze artikelen gelden wel voor algoritmische toepassingen en AI-systemen die Opdrachtnemer zelf ontwikkelt, inbrengt of levert als onderdeel van de dienstverlening, zoals eigen detectiemodellen, analysetools of automatisering. Eis 6.9 geldt in alle gevallen.
23	Programma van Eisen eis 2.8 (p. 5), 2.11 (p. 6) en 2.16 (p. 7)	Eis 2.16 houdt de Sentinel-omgeving onder de technische en administratieve zeggenschap van de gemeente. Staat de aanbestedende dienst toe dat de opdrachtnemer toegang krijgt via gedelegeerd beheer, zoals Azure Lighthouse of persoonsgebonden accounts in een Microsoft-multitenantorganisatie? Daarbij kan de gemeente die toegang op elk moment intrekken en blijft elke handeling herleidbaar tot één persoon (eis 2.8 en 2.11).	Ja. De voorkeur is om hiervoor gebruik te maken van GDAP.
24	Aanbestedingsdocument §4.2 onder d (p. 17) en §5.1.1 (p. 24); Programma van Eisen eis 8.1 (p. 21); Bijlage A1, SLA1 en SLA8	De inschrijving bevat verplicht een concept-SLA. Het Programma van Eisen en Bijlage A1 definiëren prioriteiten en doorlooptijden, maar noemen geen termijnen per prioriteit. Bevestigt de aanbestedende dienst dat: a) de inschrijver de termijnen per prioriteit zelf voorstelt in de concept-SLA; en b) de concept-SLA niet meetelt voor de maximaal acht A4 van §5.1.1? Kan zij daarnaast aangeven of de concept-SLA meeweegt in de beoordeling van de gunningscriteria, en zo ja bij welk criterium?	a) De inschrijver dient in de concept-SLA de in Bijlage A1 opgenomen termijnen per prioriteit over te nemen. De concept-SLA werkt deze termijnen uit in de meet- en uitvoeringsafspraken, zonder daarvan af te wijken. Daarnaast gelden de normen uit eisen 8.13 en 8.14 van het Programma van Eisen. b) De limiet van maximaal acht A4 geldt volgens §5.1.1 voor de uitwerking van gunningscriteria A, B en C. De concept-SLA is een afzonderlijk verplicht in te dienen document en valt niet onder deze limiet. De concept-SLA is geen zelfstandig gunningscriterium. De inschrijving wordt beoordeeld aan de hand van de gepubliceerde gunningscriteria A tot en met D. De concept-SLA wordt niet afzonderlijk beoordeeld of gescoord. De daarin beschreven aanpak kan uitsluitend worden betrokken voor zover deze relevant is voor een van de gepubliceerde beoordelingsaspecten.
25	Bijlage A1, SLA8 (doorlooptijden)	Bijlage A1 definieert de detectietijd als "de tijd tussen het optreden van een beveiligingsincident en de detectie en classificatie door het SOC". Het moment van optreden is vaak pas achteraf vast te stellen. De aanlevertijd van logdata hangt bovendien deels af van de logbronnen en van Microsoft. Is de aanbestedende dienst bereid de detectietijd te meten vanaf het moment waarop een melding in Microsoft Sentinel ontstaat?	De detectie-tijd wordt gerekend vanaf het moment dat een event die leid tot de alert in het edge-systeem (lees Active Directory, Firewall, EntraID, etc.) gegenereerd wordt. en stopt wanneer de alert ook in het SIEM voor het SOC beschikbaar komt. Enige afwijking wordt tot op bepaalde hoogte geaccepteerd in 8.22, 8.13, 8.14.

26	Bijlage A1, SLA26; Programma van Eisen eis 8.6 (p. 21) en 8.8–8.10 (p. 22); GIBIT 2025 art. 10.12 en 10.13	De boeteclausule koppelt “twee of meer per maand” per prioriteit aan een boete van 25% tot 100% van de maandelijkse kosten. Kan de aanbestedende dienst verduidelijken: a) twee of meer wát: overschrijdingen van een servicenorm, of incidenten van die prioriteit; b) of boetes van verschillende prioriteiten optellen, en tot welk maximum per maand; en c) of overschrijdingen die niet aan de opdrachtnemer toe te rekenen zijn buiten de boete vallen, zoals uitval van logbronnen of Microsoft-diensten (vergelijk eis 8.6)? Is de aanbestedende dienst daarnaast bereid pas een boete op te leggen na herhaalde overschrijding zonder voldoende opvolging van het verbeterplan (eis 8.8 tot en met 8.10)? Wij stellen daarvoor een staffel voor van 5%, 10% en 15% van de maandvergoeding.	De opdrachtgever verduidelijkt dat SLA26 ziet op twee of meer toerekenbare overschrijdingen van de voor de betreffende prioriteit geldende servicenorm in een kalendermaand. Het enkele optreden van twee of meer beveiligingsincidenten van die prioriteit leidt dus niet tot een boete wanneer de opdrachtnemer de incidenten conform de overeengekomen normen afhandelt. Dit sluit aan bij de eerdere beantwoording over SLA26: een incident op zichzelf is geen tekortkoming van de opdrachtnemer. a) Met “twee of meer per maand” worden derhalve twee of meer overschrijdingen van de toepasselijke servicenorm per prioriteitscategorie bedoeld, niet het aantal incidenten als zodanig. b) De percentages in SLA26 zijn per prioriteitscategorie opgenomen. De boete wordt toegepast op de categorie waarvoor de drempel is bereikt. c) Een overschrijding die niet aan de opdrachtnemer kan worden toegerekend, geeft geen grond voor een boete. Dit geldt onder meer wanneer de oorzaak ligt in uitval van gemeentelijke systemen, logbronnen of onderliggende Microsoft-clouddiensten, tenzij de opdrachtnemer de uitval heeft veroorzaakt of onvoldoende passende maatregelen heeft getroffen, overeenkomstig eis 8.6. De opdrachtgever neemt het voorstel om de boete pas toe te passen na herhaalde overschrijding en onvoldoende opvolging van een verbeterplan niet over. De escalatie- en verbeterplanprocedure van eisen 8.8 tot en met 8.10 staat naast de boeteregeling. Ook het voorstel voor een staffel van 5%, 10% en 15% wordt niet overgenomen; de percentages in SLA26 blijven gelden. Dit antwoord verduidelijkt de koppeling van SLA26 aan tekortkomingen van de opdrachtnemer. Het beschrijft boetes niet als sanctie voor het enkele aantal beveiligingsincidenten. GIBIT 2025 artikel 10.12 bepaalt dat partijen in het kader van een verbeterplan een tijdelijke malusregeling kunnen overeenkomen voor het toerekenbaar niet voldoen aan servicelevels; artikel 10.13 laat overige rechten van de opdrachtgever onverlet.
27	Programma van Eisen eis 5.1 (p. 16); Aanbestedingsdocument §1.1.3 (p. 6) en §5.1.2 (p. 24); Bijlage F1, regel “Totaal prijs waarop u beoordeeld wordt”	Eis 5.1 spreekt van een “initiële contractduur van vier jaar”. Het aanbestedingsdocument noemt drie jaar vast met driemaal twee jaar verlenging, en het prijzenblad rekent met de implementatie plus negen keer de jaarkosten. Bevestigt de aanbestedende dienst dat de vaste looptijd drie jaar is en dat de inschrijver het prijzenblad voor negen jaar invult?	Correct, dit is inderdaad een verschrijving in eis 5.1 van het PvE. De nieuw af te sluiten overeenkomst kent, na de implementatieperiode, een vaste looptijd van drie (3) jaar en heeft een beoogde startdatum van 1 maart 2027. Na deze vaste looptijd kan de overeenkomst drie (3) maal met een periode van telkens twee (2) jaar worden verlengd. De maximale looptijd van de overeenkomst bedraagt daarmee maximaal negen (9) jaar.
28	Aanbestedingsdocument §5.1.2 (p. 24); Programma van Eisen eis 5.3 (p. 16); GIBIT 2025 art. 11.8	§5.1.2 noemt de kosten “vast gedurende de vaste looptijd”, maar geeft de opdrachtnemer ook het recht op indexering na het eerste jaar, voor het eerst per 1 januari 2028. Eis 5.3 maakt indexering bovendien afhankelijk van schriftelijke instemming van de opdrachtgever. Bevestigt de aanbestedende dienst dat de opdrachtnemer de tarieven vanaf 1 januari 2028 jaarlijks mag indexeren volgens artikel 11.8 GIBIT? Bevestigt zij ook dat de instemming uit eis 5.3 alleen de controle van de berekening betreft?	Opdrachtnemer mag de tarieven inderdaad vanaf 1 januari 2028 jaarlijks indexeren volgens artikel 11.8 GIBIT. De instemming uit eis 5.3 van het Programma van Eisen betreft alleen de controle van de berekening.
29	Bijlage F1, onderdelen “Jaarlijkse kosten logbronnen” en “Uurtarief additionele dienstverlening”; Programma van Eisen eis 5.5 (p. 16)	Het prijzenblad vraagt per logbron een prijs per eenheid maal een aantal, maar noemt geen eenheden of aantallen. Wil de aanbestedende dienst per logbron de eenheid en het aantal opgeven, zodat alle inschrijvers met dezelfde aantallen rekenen? Anders vragen wij in elk geval het aantal gebruikers, endpoints, servers en netwerkcomponenten en het gemiddelde dagelijkse logvolume. Daarnaast noemt het prijzenblad bij het uurtarief 40 fictieve uren “waarop u beoordeeld wordt”. De formule bij “Totaal prijs waarop u beoordeeld wordt” telt deze uren echter niet mee. Telt het uurtarief mee in de evaluatieprijs?	Voor de post Honeypots/Deceptietechnologie verwijst de opdrachtgever naar het antwoord op vraag 10 in deze Nota van Inlichtingen. We hebben de beschrijving in het prijsblad voor H55 aangepast. Deze telt NIET mee voor de beoordeling. Zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.

30	Aanbestedingsdocument §1.1.1 (p. 5) en §5.1.2 (p. 25); Programma van Eisen eis 2.16 (p. 7) en 5.9 (p. 17); GIBIT 2025 art. 2.5 en 3.5	Microsoft Sentinel draait in de bestaande tenant van de gemeente. Bevestigt de aanbestedende dienst dat de licentie- en verbruikskosten van Microsoft rechtstreeks voor rekening van de gemeente komen en buiten de inschrijfprijs vallen? Het gaat dan om ingestie en retentie in Sentinel en Log Analytics en om de Defender-licenties. Bevestigt de aanbestedende dienst daarnaast dat deze Microsoft-diensten onder de eigen contractrelatie van de gemeente met Microsoft vallen? Dan gelden ze niet als Derdenprogrammatuur die de opdrachtnemer levert (artikel 2.5 en 3.5 GIBIT), en ook niet als onderaannemer van de opdrachtnemer.	De gemeente bevestigt dat Microsoft Sentinel wordt ingericht binnen de bestaande Microsoft-tenant van de gemeente. De Microsoft Sentinel- en Log Analytics-kosten voor gegevensinname en retentie vallen buiten de inschrijfprijs voor de dienstverlening van de opdrachtnemer. Dit geldt ook voor eventuele aanvullende Defender-licenties die nodig zijn: licentiekosten die Microsoft aan de gemeente in rekening brengt, zijn voor rekening van de gemeente. De Microsoft-diensten worden afgenomen onder de bestaande contract- en factureringsrelatie van de gemeente met Microsoft. De enkele inrichting of het beheer van deze diensten door de opdrachtnemer brengt ze niet onder diens contractrelatie of maakt Microsoft daarmee niet tot onderaannemer van de opdrachtnemer. De gemeentelijke tenant en de zeggenschap over Sentinel blijven bij de gemeente. Microsoft-diensten en -licenties die de gemeente zelf onder haar eigen contractrelatie afneemt, vallen niet onder de door de opdrachtnemer geleverde Derdenprogrammatuur; de opdrachtnemer blijft verantwoordelijk voor zijn eigen dienstverlening en voor het transparant benoemen van eventuele Microsoft-producten of -rechten die hij zelf aan de gemeente levert.
31	Programma van Eisen eis 2.13 (p. 6), 5.6 en 5.7 (p. 17); Bijlage F1, onderdeel “Jaarlijkse kosten logbronnen”	Voor logbronnen zonder standaardconnector implementeert de opdrachtnemer na instemming van de gemeente een passende integratie (eis 2.13). Mag de inschrijver de ontwikkeling en het onderhoud van zulke integraties opnemen in de jaarlijkse kosten per logbron, in plaats van in de implementatieprijs van maximaal € 15.000 (eis 5.7)?	Nee. Eis 5.6 bepaalt dat de vaste implementatieprijs alle werkzaamheden omvat die nodig zijn om de overeengekomen initiële implementatiescope volledig, werkend en geaccepteerd op te leveren. Als een integratie zonder standaardconnector nodig is om een overeengekomen initiële logbron aan te sluiten, moeten de initiële ontwikkeling, inrichting, documentatie en test daarvan dus in de implementatieprijs zijn inbegrepen, binnen het plafond van € 15.000 uit eis 5.7. De jaarlijkse prijs per logbron mag wel de kosten omvatten voor het reguliere beheer en onderhoud van die integratie gedurende de looptijd, mits de inschrijver die kosten en de gehanteerde aannames duidelijk toelicht. De prijsopgave moet voldoen aan eis 5.9: alle noodzakelijke kosten moeten in het prijzenblad zijn opgenomen en mogen niet later aanvullend in rekening worden gebracht.
32	Programma van Eisen eis 2.2 (p. 4), 3.3 (p. 10) en 3.5 (p. 10–11)	Eis 3.3 vraagt dat bij de initiële oplevering “minimaal de overeengekomen essentiële logbronnen” zijn aangesloten. Welke van de veertien logbronnen uit eis 2.2 beschouwt de aanbestedende dienst als essentieel voor 1 maart 2027? Kan zij daarnaast aangeven: a) welke Barracuda-producten het betreft; b) op welk platform DNS en DHCP draaien; c) of SecureMe2 NIDS en Holm Security binnen de huidige licenties logdata kunnen exporteren via syslog, CEF of een API; en d) of de gemeente een server of virtuele machine voor logverzameling beschikbaar stelt?	De in 2.2 opgenomen logbronnen worden beschouwd als essentieel voor volledige dekking van de in 2.1 vastgestelde use-cases. a) Dit betreft Barracuda firewalls b) DNS en DHCP draaien op de Active Directory Domain Controllers c) Zowel Holm als Secreme2 maken gebruik van een API (waarvoor geen licenties voor nodig zijn) d) Gemeente stelt een VM beschikbaar voor logverzameling, indien nodig.
33	Aanbestedingsdocument §1.16 (p. 9–10); Programma van Eisen eis 3.3 (p. 10); Bijlage G art. 2.1 (p. 37); GIBIT 2025 art. 4.2 en 11.2	De planning voorziet in ondertekening in week 4 of 5 van 2027 en ingebruikname op 1 maart 2027. Dat laat vier à vijf weken voor de implementatie. Bevestigt de aanbestedende dienst dat: a) de ingangsdatum evenredig opschuift als de ondertekening later plaatsvindt; b) een einddatum in het implementatieplan niet fataal is in de zin van artikel 4.2 GIBIT, voor zover vertraging ontstaat doordat de gemeente of derden informatie, toegang, besluiten of medewerking niet tijdig leveren (eis 3.3); en c) de 30% die volgens artikel 11.2 GIBIT pas na integrale acceptatie opeisbaar is, alleen de eenmalige implementatievergoeding betreft?	a) De datum van 1 maart 2027 is de beoogde datum waarop de SIEM/SOC-dienstverlening operationeel in gebruik wordt genomen. Een eventuele latere contractondertekening leidt niet automatisch tot een evenredige verschuiving van deze datum. Indien de definitieve contractering later plaatsvindt en dit gevolgen heeft voor een redelijkerwijs uitvoerbare implementatieplanning, zal de Aanbestedende dienst dit beoordelen en zo nodig de planning aanpassen. b) Artikel 4.2 GIBIT 2025 blijft ongewijzigd van toepassing. De daarin bedoelde einddatum voor de Implementatie is fataal. Daarbij geldt evenwel de in eis 3.3 van het Programma van Eisen opgenomen voorwaarde dat de Aanbestedende dienst en betrokken derden de vooraf overeengekomen informatie, toegangen, besluiten en medewerking tijdig beschikbaar stellen. Vertraging die aantoonbaar het gevolg is van het niet tijdig nakomen van deze verplichtingen door de Aanbestedende dienst of betrokken derden wordt niet zonder meer aan Opdrachtnemer toegerekend. c) Voor de facturatie geldt de systematiek zoals nader verduidelijkt in het antwoord op vraag 189.

34	Bijlage A1, DIV31 en TECH42; GIBIT 2025 art. 22.8 en 33.2	Bijlage A1 eist dat de opdrachtnemer logdata in de SIEM en rapportagedata in de SOC-omgeving na maximaal één jaar vernietigt (DIV31). Dezelfde bijlage eist ook dat data niet verwijderd kunnen worden (TECH42). Artikel 22.8 en 33.2 GIBIT staan vernietiging zonder verzoek van de gemeente niet toe. Welke bewaartermijn wenst de gemeente voor logdata, binnen het maximum van één jaar? Bevestigt de aanbestedende dienst daarnaast dat: a) automatische verwijdering na afloop van een schriftelijk vastgelegde bewaartermijn geldt als vernietiging op verzoek van de gemeente; b) TECH42 betekent dat data binnen de bewaartermijn beschermd zijn tegen ongeautoriseerde wijziging of verwijdering; en c) de opdrachtnemer beknopte incidentregistraties langer dan één jaar mag bewaren als de gemeente daarmee instemt?	DIV31 bepaalt dat logdata in de SIEM-oplossing en rapportagedata in de SOC-omgeving uiterlijk één jaar na vastlegging worden vernietigd. De eis stelt daarmee een vaste bewaartermijn van één jaar en vastgelegd in de SLA/DAP en de toepasselijke verwerkingsafspraken. a) De opdrachtgever bevestigt dat automatische vernietiging na afloop van de aldus vastgelegde bewaartermijn mag plaatsvinden. De vooraf vastgelegde termijn en automatische verwijdering gelden als een schriftelijke instructie van de opdrachtgever voor die vernietiging. De opdrachtnemer legt de vernietigingsprocedure vast en kan de uitvoering daarvan aantonen. b) TECH42 betreft back-up- en herstelvoorzieningen en bepaalt dat gegevens niet verloren mogen gaan en geborgd moet zijn dat data niet verwijderd kan worden. Dit wordt gelezen in samenhang met DIV31: binnen de bewaartermijn moet de data beschermd zijn tegen ongeautoriseerde of onbedoelde wijziging en verwijdering; na afloop van de vastgelegde bewaartermijn moet de data overeenkomstig DIV31 worden vernietigd. De herstelvoorzieningen mogen de overeengekomen vernietiging niet doorkruisen. c) Nee. Op grond van DIV31 worden de genoemde logdata en rapportagedata uiterlijk na één jaar vernietigd. Bewaring van incidentregistraties langer dan één jaar is op basis van deze eis niet toegestaan, ook niet met afzonderlijke instemming. Indien voor bepaalde gegevens een wettelijke bewaarplicht of andere geldige grond bestaat, moet die uitzondering vooraf met de opdrachtgever worden afgestemd en schriftelijk worden vastgelegd.
35	GIBIT 2025 art. 1.27, 17.4 en 18.2; Aanbestedingsdocument §5.1.2 (p. 24); Bijlage F	Artikel 1.27 GIBIT berekent de Jaarvergoeding door “de Vergoeding te delen door de initieel beoogde looptijd van de Overeenkomst in jaren”. Het inschrijvingsbiljet vraagt de totaalprijs voor negen jaar, terwijl de initiële looptijd drie jaar is. Bevestigt de aanbestedende dienst dat de Jaarvergoeding gelijk is aan de gemiddelde vergoeding per contractjaar, en niet aan de negenjaarsprijs gedeeld door drie? Is de aanbestedende dienst daarnaast bereid in artikel 17 GIBIT indirecte schade en gevolgschade uit te sluiten, waaronder gederfde winst, behalve bij opzet of grove schuld?	De Aanbestedende dienst bevestigt dat de Jaarvergoeding gelijk is aan de gemiddelde vergoeding per contractjaar en niet aan de negenjaarsprijs gedeeld door drie. Indirecte schade en gevolgschade worden niet uitgesloten. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
36	Programma van Eisen eis 2.23 (p. 8) en 6.3 (p. 18); Aanbestedingsdocument §1.1.1 (p. 6); GIBIT 2025 art. 1.31, 21.4 en 21.5	Eis 2.23 en 6.3 maken de gemeente eigenaar van klantspecifieke detectieregels, playbooks en configuraties, en geven haar voor generieke componenten van de opdrachtnemer een gebruiksrecht. Het gaat hier om generieke detectieregels, playbooks en automatiseringen die de opdrachtnemer al bezit en bij meerdere klanten inzet. Bevestigt de aanbestedende dienst dat die ook na plaatsing in de tenant van de gemeente eigendom blijven van de opdrachtnemer, onder het gebruiksrecht uit eis 2.23? En dat ze geen Maatwerkprogrammatuur zijn in de zin van artikel 1.31, 21.4 en 21.5 GIBIT?	Ja. Reeds vóór de opdracht bestaande, generieke detectieregels, playbooks en automatiseringen van de opdrachtnemer blijven eigendom van de opdrachtnemer, ook wanneer deze in de Microsoft Sentinel-tenant van de gemeente worden geplaatst. De gemeente krijgt daarop het in eis 2.23 bedoelde gebruiksrecht voor de uitvoering, continuïteit en overdracht van de dienstverlening. Plaatsing in de gemeentelijke tenant brengt op zichzelf geen eigendomsoverdracht mee. Dit geldt niet voor onderdelen die specifiek voor de gemeente worden ontwikkeld of aangepast. De gemeente blijft op grond van eisen 2.23 en 6.3 eigenaar van de klantspecifieke resultaten en configuraties die binnen de opdracht worden gerealiseerd. De opdrachtnemer kan voor de reeds bestaande generieke componenten in beginsel een beroep doen op de GIBIT-bepalingen over intellectuele eigendom. Of een onderdeel als Maatwerkprogrammatuur kwalificeert, wordt echter bepaald aan de hand van de definitie in artikel 1.31 GIBIT 2025: het moet specifiek voor de opdrachtgever, in diens schriftelijke opdracht en voor diens kosten zijn ontwikkeld; voor een aanpassing of inrichting van standaardprogrammatuur is daarbij ook van belang of de broncode wordt aangepast. De generieke componenten zoals hierboven beschreven voldoen daar niet aan. De artikelen 21.4 en 21.5 moeten in samenhang met die definitie en de concrete aard van het betreffende onderdeel worden toegepast.

37	Bijlage A1, A28–A34, TECH24, TECH25 en TECH57; Nota van Inlichtingen 1 (20-10-2026)	In de Nota van Inlichtingen van 20 oktober 2026 laat de aanbestedende dienst eis TECH13 vervallen, omdat die per abuis in Bijlage A1 was blijven staan. Bijlage A1 bevat meer eisen die lijken bedoeld voor een softwarepakket. Voorbeelden zijn “een app voor gebruik op een Android Smartphone, iPhone of iPad” (TECH25), “Alle wettelijk verplichte toekomstige modules zijn inbegrepen in de opdracht” (A30) en “Indien maatwerk nodig is, wordt dit direct gezien als onderdeel van de standaard” (A34). Kan de aanbestedende dienst aangeven welke eisen uit Bijlage A1 gelden voor deze dienstverlening in de eigen Microsoft-tenant van de gemeente? Bevestigt zij in elk geval dat: a) toegang via de webportalen van Microsoft en de opdrachtnemer op mobiele apparaten voldoet aan TECH25; en b) A34 niet betekent dat aanvullende use cases op verzoek van de gemeente kosteloos zijn, nu het prijzenblad die als aparte prijscomponent opneemt?	Wijzigingen Bijlage A1 – Programma van Eisen non-functionals TECH13 vervalt. Een ISO 20000-certificaat of vergelijkbaar wordt niet verlangd. Eis 1.4 van het Programma van Eisen blijft onverkort van toepassing. TECH25 vervalt. De toegangseisen uit eisen 2.7 en 2.25 van het Programma van Eisen blijven onverkort van toepassing. A30: De prijzen omvatten de dienstverlening voor de in de aanbestedingsstukken genoemde use-cases (eis 2.1) en de passende aanvullende use-cases voor de in eis 2.2 genoemde logbronnen. Use-cases die niet in de aanbestedingsstukken zijn genoemd en niet draaien op de in eis 2.2 genoemde logbronnen, vallen buiten de scope van deze opdracht. Het toevoegen daarvan gebeurt als meerwerk conform eis 5.10. A34 Maatwerk dat binnen de tenant van Opdrachtgever wordt gerealiseerd, zoals detectieregels, queries, playbooks, workbooks en connectorconfiguraties, is eigendom van Opdrachtgever (zie ook eisen 2.23 en 6.3). Maatwerk of aanvullende voorzieningen buiten de tenant van Opdrachtgever worden uitsluitend ingezet na voorafgaand overleg met en schriftelijke goedkeuring van Opdrachtgever.
38	Aanbestedingsdocument §5.1.1 (p. 20–24) en §3.2.1 (p. 15); Bijlage E	Voor subgunningscriterium A, B en C zijn samen maximaal acht A4 beschikbaar. Criterium A vraagt een planning met activiteiten, afhankelijkheden en verantwoordelijken, en criterium B een RACI-model. Mag de inschrijver de planning en het RACI-model als bijlage indienen, buiten de acht A4? Tellen een voorblad en inhoudsopgave mee? Mag de inschrijver daarnaast de beveiligingsmaatregelen voor werk buiten de SOC-locatie (kerncompetentie 2) in een bijlage bij Bijlage E beschrijven, buiten de 1.000 woorden?+D162	Ja dit zijn inderdaad 8 inhoudelijke pagina's en het is dus akkoord dat dit exclusief voorblad, inhoudsopgave en eventuele bijlage(s) is. Als bijlagen buiten de acht inhoudelijke A4 mogen uitsluitend de planning en het RACI-model worden toegevoegd. De inschrijver mag daarnaast de beveiligingsmaatregelen voor werk buiten de SOC-locatie (kerncompetentie 2) in een bijlage bij Bijlage E beschrijven, buiten de 1.000 woor
39	Bijlage G art. 2.1-2.2 (p.37) Leidraad §1.1.3 (p.6) PvE A, eis 5.1 (p.16)	Artikel 2.1 van bijlage G bepaalt expliciet dat de initiële looptijd drie jaar bedraagt (1 maart 2027 tot en met 28 februari 2030), met op grond van artikel 2.2 maximaal drie verlengingen van twee jaar. Eis 5.1 van bijlage A noemt daarentegen een initiële looptijd van vier jaar. Kan de aanbestedende dienst bevestigen dat deze vermelding van vier jaar een verschrijving betreft en de eis, alsmede eventuele daarmee samenhangende prijsinstructies, dienovereenkomstig aanpassen?	Correct, dit is inderdaad een verschrijving in eis 5.1 van het PvE. De nieuw af te sluiten overeenkomst kent, na de implementatieperiode, een vaste looptijd van drie (3) jaar en heeft een beoogde startdatum van 1 maart 2027. Na deze vaste looptijd kan de overeenkomst drie (3) maal met een periode van telkens twee (2) jaar worden verlengd. De maximale looptijd van de overeenkomst bedraagt daarmee maximaal negen (9) jaar.
40	Leidraad §5.1.2 (pp.24–25) Bijlage F1, cellen F11, F37 en F40 Bijlage G art. 2–3 (p.37) PvE A eis 5.1 (p.16)	Paragraaf 5.1.2 schrijft een inschrijfsom over de maximale looptijd van negen jaar voor. Het prijzenblad berekent in F40 de beoordelingsprijs als F11 (eenmalige kosten) plus negenmaal F37 (jaarlijkse basiskosten), terwijl eis 5.1 van bijlage A nog spreekt over vier jaar. Kan de gemeente bevestigen dat de uitkomst van F40 leidend is voor de aanneemsom op het inschrijvingsbiljet en dat de negenjaarsberekening geldt, ongeacht de gefaseerde verlengingsopties?	Correct, dit is inderdaad een verschrijving in eis 5.1 van het PvE. De nieuw af te sluiten overeenkomst kent, na de implementatieperiode, een vaste looptijd van drie (3) jaar en heeft een beoogde startdatum van 1 maart 2027. Na deze vaste looptijd kan de overeenkomst drie (3) maal met een periode van telkens twee (2) jaar worden verlengd. De maximale looptijd van de overeenkomst bedraagt daarmee maximaal negen (9) jaar.

41	Leidraad §5.1.2 (p.24); Bijlage F1 F40; Bijlage G art. 3 (p.37); PvE A eis 5.3 (p.16); GIBIT art. 11.8–11.9 (pp.17–18)	Paragraaf 5.1.2 noemt enerzijds vaste tarieven gedurende de initiële looptijd, maar staat anderzijds indexering vanaf 1 januari 2028 toe. In bijlage G ontbreekt een zelfstandige indexeringsbepaling, terwijl het prijzenblad in F40 met negen ongewijzigde jaarbedragen rekent. Kan de gemeente bevestigen dat GIBIT artikel 11.8 (met inachtneming van artikel 11.9) van toepassing is op de tarieven vanaf de genoemde datum en dat de beoordelingsprijs wordt berekend op basis van ongeïndexeerde nominale tarieven over negen jaar?	Opdrachtnemer mag de tarieven inderdaad vanaf 1 januari 2028 jaarlijks indexeren volgens artikel 11.8 GIBIT. De instemming uit eis 5.3 van het Programma van Eisen betreft alleen de controle van de berekening.
42	Bijlage F1, rijen 13–40 Leidraad §1.1.1 (pp.5–6) PvE A eisen 2.16 en 5.5 (pp.7,16)	Worden Microsoft Sentinel-, Log Analytics-, Logic Apps- en overige Azure-verbruikskosten rechtstreeks door Opdrachtgever gedragen of moeten deze kosten in de inschrijfsom worden opgenomen?	De Microsoft Sentinel-omgeving wordt ingericht binnen de bestaande Microsoft-tenant van de gemeente. Azure-verbruikskosten die rechtstreeks voortvloeien uit het gebruik van Microsoft Sentinel, Log Analytics, Logic Apps en andere Azure-resources vallen daarom niet onder de inschrijfsom van de opdrachtnemer, maar worden door de gemeente gedragen via de toepasselijke Microsoft-factureringsrelatie.
43	Bijlage F1, kolommen D–E, rijen 14–36 PvE A eisen 2.1–2.2 en 5.5 (pp.4,16) Leidraad §3.2.1 (p.15)	Welke bindende beoordelingsaantallen moeten inschrijvers per logbron in Bijlage F1 hanteren?	Prijzenblad bevat nu beoordelingsaantallen. Zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.
44	Bijlage F1, rijen 14–27 PvE A eisen 2.2 en 3.3 (pp.4,10)	Eis 2.2 noemt veertien logbronnen, die eveneens in bijlage F1, rijen 14 tot en met 27, zijn opgenomen. Eis 3.3 verlangt bij livegang de aansluiting van de 'overeengekomen essentiële logbronnen'. Welke van deze veertien logbronnen moeten uiterlijk op 1 maart 2027 operationeel zijn aangesloten en geaccepteerd, en welke mogen gefaseerd tijdens de beheerperiode worden toegevoegd?	De opdrachtgever verduidelijkt dat alle veertien in eis 2.2 genoemde logbronnen onderdeel zijn van de initiële scope en uiterlijk bij de initiële oplevering aangesloten, getest, operationeel en geaccepteerd moeten zijn. Gefaseerde aansluiting ná ingebruikname voldoet niet aan de vereiste initiële scope.
45	PvE A, eisen 2.2 en 2.13 (pp.4,6)	Voor de genoemde Microsoft- en niet-Microsoft-bronnen worden passende aanvullende use-cases “out of the box” verlangd, terwijl eis 2.13 expliciet een alternatieve integratiemethode toestaat als een standaardconnector ontbreekt. Wordt een aantoonbaar werkende, ondersteunde API- of maatwerkkoppeling met bijbehorende use-cases als gelijkwaardig aan “out of the box” geaccepteerd?	Een aantoonbaar werkende en ondersteunde integratie via een API of een andere passende integratiemethode kan worden geaccepteerd wanneer voor een logbron geen standaardconnector beschikbaar is. Dit volgt uit eis 2.13. De integratie moet de logbron betrouwbaar aansluiten op Microsoft Sentinel en de overeengekomen aanvullende use-cases ondersteunen. De inschrijver beschrijft hoe de koppeling werkt, wordt getest en onderhouden, en vermeldt eventuele afhankelijkheden. Als voor deze aansluiting maatwerk nodig is, geldt op grond van eis A34, bijlage A1 dat dit onderdeel wordt van de standaard aangeboden ICT-prestatie. De ontwikkeling en het reguliere onderhoud van de noodzakelijke maatwerkkoppeling mogen daarom niet als een afzonderlijke maatwerkprestatie buiten de aangeboden standaardprestatie worden geplaatst. De implementatie vindt plaats na instemming van de opdrachtgever en overeenkomstig de overeengekomen scope en prijsafspraken.
46	PvE A, eisen 2.1 en 3.3 (pp.4,10)	Wat zijn de concrete acceptatiecriteria voor de vijf initiële use-cases (UC1 tot en met UC5), bijvoorbeeld verplichte scenario’s, benodigde gegevensbronnen, testmethode, detectiegrenswaarden en toelaatbare false positives? Worden deze criteria voorafgaand aan implementatie gezamenlijk vastgesteld en binnen de overeengekomen scope gehouden?	De eisen noemen de vijf initiële use-cases en beschrijven per use-case het beoogde detectiedoel. Zij schrijven echter geen uitputtende lijst voor van verplichte scenario’s, detectiegrenswaarden of een maximaal percentage false positives. De opdrachtnemer werkt, aan de hand van het Implementatieplan, de use-cases tijdens de implementatie samen met de opdrachtgever uit. Daarbij worden onder meer de relevante scenario’s, benodigde en beschikbare logbronnen, detectielogica, testmethode en acceptatiecriteria vastgesteld. De uitwerking wordt gedocumenteerd en getest; de opdrachtgever accepteert de vijf use-cases vóór de ingebruikname, overeenkomstig eis 3.3. Klantspecifieke detecties worden in samenwerking opgesteld en pas na de overeengekomen test en autorisatie in productie genomen. De uitwerking blijft binnen de overeengekomen initiële scope en de vijf beschreven use-cases. Aanvullende use-cases of wezenlijke uitbreidingen daarvan worden behandeld volgens de daarvoor geldende afspraken en prijscomponent in het prijzenblad. Deze werkwijze verduidelijkt de implementatie en acceptatie, maar wijzigt de vereiste initiële scope niet.

47	Bijlage F1, rijen 8–11, cel F9; PvE A, eisen 3.2, 3.3 en 5.6–5.7 (pp. 10, 17)	Eis 5.7 maximeert alle implementatiekosten op € 15.000,-, terwijl eis 5.6 onder meer het ontwerp, de volledige Sentinel-inrichting, de koppeling van alle logbronnen, de implementatie van vijf use-cases, testen, documentatie, opleiding en de stabilisatiefase omvat. In bijlage F1 is bovendien uitsluitend één gezamenlijke invoerregel (F9) opgenomen voor deze totale inspanning. Kan de gemeente aangeven welke activiteiten en eventuele licentie- of werkzaamheden van bestaande ICT-leveranciers onder dit plafond vallen? Is de gemeente, gelet op de omvang van de gevraagde opleveringen, bereid dit plafond te heroverwegen of te bevestigen dat niet-voorziene maatwerkkoppelingen en uitbreidingen na acceptatie via het wijzigingsproces afzonderlijk worden vergoed?	Het plafond van € 15.000 exclusief btw is van toepassing op de totale implementatieprijs. Deze vaste prijs omvat de activiteiten die nodig zijn om de overeengekomen initiële implementatiescope volledig, werkend en geaccepteerd op te leveren, zoals genoemd in eis 5.6: projectmanagement, ontwerp, inrichting en configuratie van Microsoft Sentinel, aansluiting van de overeengekomen initiële logbronnen, implementatie en acceptatie van de vijf initiële use-cases, inrichting van de SOC-dienstverlening, documentatie, opleiding, testen, herstel van bevindingen en ondersteuning tijdens de stabilisatieperiode. Deze kosten worden ingevuld op de gezamenlijke prijsregel in Bijlage F1. Het plafond omvat ook alle initiële werkzaamheden en kosten die nodig zijn om aan de overeengekomen scope te voldoen, waaronder de noodzakelijke werkzaamheden van de opdrachtnemer voor koppelingen en afstemming met bestaande ICT-leveranciers. Kosten die naar hun aard behoren tot de structurele dienstverlening mogen niet uitsluitend of onevenredig als implementatiekosten worden opgevoerd. Eventuele licentie- of verbruikskosten van Microsoft die rechtstreeks door de gemeente worden gedragen, vallen niet onder de implementatieprijs. Het plafond wordt niet heroverwogen. Inschrijvers moeten de volledige initiële scope aanbieden binnen de vaste implementatieprijs van maximaal € 15.000. Werkzaamheden die uitsluitend betrekking hebben op uitbreidingen buiten de overeengekomen initiële scope kunnen alleen als meerwerk worden uitgevoerd na voorafgaande schriftelijke opdracht van de opdrachtgever. Werkzaamheden die nodig zijn om de overeengekomen initiële scope alsnog volledig, werkend en geaccepteerd op te leveren, vallen onder de vaste implementatieprijs en kunnen niet afzonderlijk in rekening worden gebracht. Zie ook vraag 14 met daarin meer beschrijving over de training.
48	Leidraad §1.16 (p.10) PvE A, eisen 3.3 en 3.5 (pp.10-11)	De overeenkomst wordt naar verwachting in week 4 of 5 van 2027 getekend en de oplossing moet 1 maart 2027 in productie zijn. Welke minimale beschikbaarheid van toegang, tenantrechten, informatie, testcapaciteit en medewerking van bestaande leveranciers garandeert de gemeente vanaf contractondertekening, en hoe wordt de datum aangepast als deze randvoorwaarden niet tijdig worden vervuld?	De gemeente stelt de voor de implementatie benodigde informatie, besluiten, toegangen en medewerking tijdig beschikbaar, en coördineert waar nodig de medewerking van betrokken gemeentelijke leveranciers. De concrete randvoorwaarden, benodigde tenantrechten, testcapaciteit, verantwoordelijkheden en afhankelijkheden moeten worden vastgelegd in het implementatieplan, overeenkomstig eis 3.5. De opdrachtgever verstrekt de overeengekomen toegangen en autorisaties voor de gemeentelijke tenant; werkzaamheden aan gemeentelijke systemen waarvoor de opdrachtnemer geen toegang of bevoegdheid heeft, worden door de gemeente of de betreffende ICT-dienstverlener uitgevoerd, op basis van tijdige instructies en ondersteuning van de opdrachtnemer. Eis 3.3 bepaalt dat de opdrachtnemer de dienstverlening uiterlijk 1 maart 2027 operationeel oplevert, onder de voorwaarde dat de opdrachtgever en betrokken derden de vooraf overeengekomen informatie, toegangen, besluiten en medewerking tijdig beschikbaar stellen. De opdrachtnemer moet een dreigende vertraging direct melden, met oorzaak, gevolgen en beheersmaatregelen. De aanbestedingsstukken bepalen niet dat de datum automatisch verschuift zodra een randvoorwaarde niet tijdig is vervuld. Partijen bespreken in dat geval de gevolgen voor de planning en leggen eventuele aanpassing schriftelijk vast. Een wijziging van de overeengekomen datum is dus niet automatisch en kan niet eenzijdig worden aangenomen.

49	Bijlage F1, rij 48 (CERT/IR) PvE A eisen 4.12 en 5.9 (pp.13,17) Leidraad §1.1.1 (p.5)	Welke incidentresponsewerkzaamheden (zoals diepgaand forensisch onderzoek, containment en eerste herstelondersteuning) zijn verplicht inbegrepen in de vaste SOC-vergoeding, en welke behoren tot de optionele 'CERT Dienstverlening en IR Retainers' in rij 48 van bijlage F1? Kan de gemeente de minimale inbegrepen inzet en 24/7-beschikbaarheid per incident specificeren om de verplichte en optionele scope eenduidig te onderscheiden?	De vaste SOC-vergoeding omvat de reguliere SOC-dienstverlening zoals omschreven in het Programma van Eisen, waaronder 24/7 ontvangst en verwerking van beveiligingsmeldingen, triage, analyse, classificatie, tijdige melding en escalatie, en het leveren van een eerste bruikbare analyse en advies binnen de overeengekomen termijnen. Ook beschikt de opdrachtnemer over voldoende gekwalificeerde capaciteit om bij kritieke en hoge incidenten tijdig aanvullende analyse en ondersteuning te leveren (eis 4.12). De aanbestedingsstukken leggen geen vaste minimale inzet in uren of een vaste duur van incidentresponse per incident vast. De inschrijver moet in de concept-SLA en het prijzenblad duidelijk aangeven welke incidentresponsewerkzaamheden in de vaste SOC-vergoeding zijn inbegrepen, welke inzet, starttermijnen en beschikbaarheid daarvoor gelden, en welke specialistische dienstverlening daarbuiten valt en onder de optionele post ‘CERT Dienstverlening en IR Retainers’ in Bijlage F1 wordt aangeboden. Dit betreft onder meer de afbakening van diepgaand forensisch onderzoek, uitgebreide containment en eerste herstelondersteuning. Inzet op locatie vindt alleen plaats als dit afzonderlijk is overeengekomen of als optionele dienstverlening wordt afgenomen. De gemeente stelt in de aanbestedingsstukken geen aanvullende uniforme minimumuren of maximale inzet per incident vast. De inschrijver dient die reikwijdte en eventuele kosten transparant te beschrijven. Kosten die nodig zijn om aan de eisen en de aangeboden vaste SOC-dienstverlening te voldoen, zijn inbegrepen in de inschrijfprijs, tenzij het prijzenblad een onderdeel uitdrukkelijk als afzonderlijke of optionele prijscomponent aanwijst (eis 5.9). De optionele post wordt alleen afgenomen na opdracht van de gemeente.
50	Leidraad §3.2.1, KC1 en KC2 (p.15)	Beide kerncompetenties vereisen een referentie bij een gemeentelijke organisatie met ten minste 420 gebruikers. Welke inhoudelijke kenmerken maken gemeentelijke ervaring noodzakelijk en kan aantoonbaar gelijkwaardige ervaring bij andere (semi)publieke organisaties met vergelijkbare hybride complexiteit en beveiligingsvereisten eveneens worden geaccepteerd?	De Aanbestedende dienst handhaaft de eis dat de referentie betrekking heeft op een gemeentelijke organisatie met ten minste 420 gebruikers. Hiermee wordt beoogd ervaring aan te tonen met SIEM/SOC-dienstverlening binnen de specifieke gemeentelijke ICT-context, waaronder de organisatorische inrichting, informatiebeveiliging en voor gemeenten relevante wettelijke en beleidsmatige kaders. Ervaring bij andere (semi)publieke organisaties wordt daarom niet als vervanging voor de gevraagde gemeentelijke referentie geaccepteerd.
51	Leidraad §3.2.1 en §3.2.1.1 (p.15) Bijlage E (p.1)	Kerncompetenties vereisen uitvoering én oplevering van een opdracht in de afgelopen drie jaar, terwijl SOC-diensten vaak doorlopend worden geleverd. Wordt een lopende referentieovereenkomst geaccepteerd wanneer de implementatie aantoonbaar is opgeleverd en de SOC-dienstverlening gedurende de referentieperiode succesvol en aantoonbaar is uitgevoerd?	Ja dat is correct.
52	Bijlage A1, eis SLA26 (p.4); PvE A, eisen 8.8–8.14 (pp.22–23); GIBIT art. 10.12–10.13 (pp.15–16)	Eis SLA26 verbindt aan "twee of meer" P1-, P2-, P3- of P4-incidenten per maand boetes van respectievelijk 100%, 50%, 25% en 25% van de maandelijkse vergoeding. Het enkele aantal beveiligingsincidenten zegt echter niets over een toerekenbare tekortkoming van de SOC-leverancier. Inschrijver acht een op incidentaantallen gebaseerde boeteregeling disproportioneel voor managed-securitydienstverlening. Bent u bereid SLA26 te verwijderen? Zo nee, wilt u deze beperken tot aantoonbaar aan opdrachtnemer toerekenbare overschrijdingen van concreet overeengekomen SLA-normen en de grondslag van "twee of meer" expliciet definiëren?	De opdrachtgever verwijdert SLA26 niet. Het enkele optreden of aantal beveiligingsincidenten van een bepaalde prioriteit leidt niet tot een boete wanneer de opdrachtnemer de overeengekomen dienstverlening en servicenormen naleeft. SLA26 wordt verduidelijkt: met “twee of meer per maand” worden twee of meer aantoonbare, aan de opdrachtnemer toerekenbare overschrijdingen van de voor de betreffende prioriteit geldende servicenorm bedoeld, niet twee of meer incidenten als zodanig. Overschrijdingen die niet aan de opdrachtnemer zijn toe te rekenen, waaronder de situaties omschreven in eis 8.6, tellen niet mee. De in SLA26 genoemde percentages blijven ongewijzigd: 100% voor Prio 1, 50% voor Prio 2 en 25% voor Prio 3 en Prio 4. Het voorstel om SLA26 te verwijderen wordt niet overgenomen. De escalatie- en verbeterplanprocedure van eisen 8.8 tot en met 8.10 blijft van toepassing. Die procedure staat naast de verduidelijkte boeteregeling: een verbeterplan is niet als afzonderlijke voorwaarde opgenomen voordat een boete kan worden toegepast.

53	Bijlage A1, eisen SLA1.2 en SLA26 (p.4); GIBIT art. 10.12–10.13 en 17 (pp.15–16,21)	Kunnen boetes uit SLA26 per maand cumuleren over meerdere prioriteiten of SLA-normen en, zo ja, tot welk absoluut maximum? Hoe worden deze verrekend met servicecredits, verbetermaatregelen en schadevergoeding onder de GIBIT? Is de gemeente bereid een proportioneel gezamenlijk maandplafond op te nemen en te bevestigen dat op grond van GIBIT artikel 10.12 tijdens de uitvoering geen aanvullende financiële sancties worden ingevoerd zonder voorafgaande uitdrukkelijke schriftelijke instemming van beide partijen?	De opdrachtgever bevestigt dat SLA26 ziet op twee of meer aantoonbare en aan de opdrachtnemer toerekenbare overschrijdingen van de voor de betreffende prioriteit geldende servicenorm in een kalendermaand. Het enkele aantal incidenten leidt niet tot een boete. Daarmee wordt aangesloten bij de eerdere verduidelijking dat een beveiligingsincident op zichzelf geen tekortkoming van de SOC-leverancier vormt. De aanbestedingsstukken bepalen niet expliciet of boetes voor verschillende prioriteiten cumuleren, noch welk gezamenlijk maximum per maand geldt. Om hierover geen nieuwe financiële voorwaarde te introduceren, wordt in deze Nota geen cumulatie- of maandmaximum toegevoegd. De definitieve SLA dient de toepassing van SLA26, waaronder eventuele samenloop bij meerdere prioriteiten, expliciet en eenduidig uit te werken. Niet-toerekenbare overschrijdingen vallen buiten de boetegrondslag. De escalatie- en verbeterplanprocedure van eisen 8.8–8.10 blijft daarnaast gelden. De opdrachtgever neemt het voorstel voor een gezamenlijk maandplafond op dit moment niet over. Op grond van GIBIT 2025 artikel 10.12 kunnen partijen in het kader van een verbeterplan een tijdelijke malusregeling overeenkomen voor het toerekenbaar niet voldoen aan servicelevels. Artikel 10.13 bepaalt dat een dergelijke regeling en eventueel in de SLA bedongen maatregelen de overige rechten van de opdrachtgever onverlet laten; betaalde boetes worden overeenkomstig de GIBIT in mindering gebracht op een schadevergoeding.
54	Bijlage A1, eis SLA8 (p.4) PvE A, eis 8.6 (p.21)	Bij SLA8 begint de detectietijd bij het optreden van een incident, terwijl het SOC het incident pas kan detecteren nadat de relevante telemetrie is gegenereerd en beschikbaar is gekomen. Kan de detectietijd worden gemeten vanaf aantoonbare ontvangst van de relevante melding/logdata in de overeengekomen keten, met een afzonderlijke norm voor logbrongezondheid en vertraging?	De opdrachtgever verwijst naar het antwoord op vraag 25 in deze Nota van Inlichtingen.
55	Bijlage A1, eis SLA8 (p.4) PvE A, eisen 8.13-8.14 (p.22)	Bijlage A1 noemt per incidentprioriteit concrete detectie-, reactie- en escalatietijden, terwijl bijlage A, eisen 8.13 en 8.14, een realisatiepercentage van minimaal 95% voorschrijft. Zijn de tijden uit SLA8 individuele resultaatsverplichtingen voor 100% van de meldingen of meetwaarden waarop de 95%-norm per meetperiode wordt toegepast?	De termijnen in Bijlage A1 bij SLA8 zijn de overeengekomen normwaarden per incident en prioriteit. De verplichting om deze termijnen te halen geldt dus voor iedere melding. De 95%-normen in eisen 8.13 en 8.14 vormen daarnaast de meetbare prestatienormen voor de dienstverlening over de betreffende rapportageperiode: minimaal 95% van de meldingen moet binnen de toepasselijke meldtijd aan de opdrachtgever worden gemeld, en voor minimaal 95% van de incidenten moet tijdig een eerste bruikbare analyse en advies worden geleverd. De 95%-norm is daarmee geen toestemming om de SLA-termijn bij de overige meldingen te overschrijden; zij bepaalt wanneer aan de afzonderlijke prestatienorm voor tijdige melding respectievelijk eerste analyse en advies is voldaan. De registratie, meetperiode en berekeningswijze worden in de SLA vastgelegd. Alle overschrijdingen blijven zichtbaar in de rapportage en kunnen aanleiding geven tot de escalatie- en verbeterplanprocedure van eisen 8.8–8.10.
56	Bijlage A1, eisen SLA18 en TECH42 (p.2) PvE A, eis 8.6 (p.21)	TECH42 verlangt herstel binnen 24 uur na een ramp of incident buiten de invloed van opdrachtnemer en stelt dat geen gegevens verloren mogen gaan. Op welke door opdrachtnemer beheerde componenten ziet dit, en geldt de eis van nul gegevensverlies ook voor Microsoft Sentinel en gemeentelijke brondata buiten de feitelijke zeggenschap van opdrachtnemer? Welke RPO- en RTO-waarden zijn afzonderlijk van toepassing?	TECH42 geldt voor de onderdelen van de ICT-prestatie waarvoor de opdrachtnemer verantwoordelijk is en waarvoor hij back-up- en herstelvoorzieningen kan inrichten zoals bijvoorbeeld een door de opdrachtnemer beheerd SOC-portaal en bijbehorende rapportage- of supportomgeving. De eis houdt in dat deze onderdelen na een ramp of incident buiten de invloed van de opdrachtnemer binnen 24 uur weer operationeel zijn en dat geborgd is dat gegevens niet verloren gaan of ongeautoriseerd verwijderd kunnen worden. Microsoft Sentinel draait volgens eis 2.16 in de bestaande Microsoft-tenant van de gemeente. De gemeente blijft verantwoordelijk voor de tenant en voor gemeentelijke brondata in systemen die de opdrachtnemer niet beheert. TECH42 legt de opdrachtnemer daarom geen garantie op voor herstel of nul gegevensverlies van Microsoft-diensten of gemeentelijke brondata buiten zijn feitelijke zeggenschap. De opdrachtnemer blijft wel verantwoordelijk voor passende continuïteits-, back-up- en herstelmaatregelen voor de door hem beheerde onderdelen van de SOC-dienstverlening en voor de naleving van eis 8.6 ten aanzien van monitoring van logbronnen en het signaleren en melden van uitval. De aanbestedingsstukken noemen geen afzonderlijke RPO-waarde of aanvullende RTO-waarde. Voor de onder TECH42 vallende onderdelen geldt de expliciete eis dat de dienstverlening binnen 24 uur wordt hervat; een afzonderlijke RPO wordt niet gespecificeerd. De concrete verdeling van verantwoordelijkheden en eventueel toepasselijke hersteldoelen voor Microsoft Sentinel en gemeentelijke brondata worden in het continuïteits- en herstelplan en het DAP vastgelegd.

57	Bijlage A1, eis SLA15 (p.2) PvE A, eis 8.6 (p.21)	Bijlage A1 formuleert een algemene beschikbaarheid van 99,9% voor de ICT-prestatie; eis 8.6 van bijlage A beperkt de garantie tot door opdrachtnemer beheerde onderdelen met uitzonderingen voor niet-toerekenbare gemeentelijke en Microsoft-storingen. Kan worden bevestigd dat deze afbakening voor beide eisen geldt en de meetmethode, geplande onderhoudsvensters en uitzonderingen in de SLA worden vastgelegd?	Ja. De opdrachtgever bevestigt dat de beschikbaarheidseis van minimaal 99,9% per kalendermaand ziet op de door de opdrachtnemer beheerde onderdelen van de SIEM/SOC-dienstverlening, zoals uitgewerkt in eis 8.6 van het Programma van Eisen. Deze afbakening geldt ook voor SLA15 in Bijlage A1. Uitval van gemeentelijke systemen, logbronnen of onderliggende Microsoft-clouddiensten wordt niet aan de opdrachtnemer toegerekend, tenzij de opdrachtnemer de uitval heeft veroorzaakt of onvoldoende passende maatregelen heeft getroffen. De meetmethode, de berekening van de beschikbaarheid, geplande onderhoudsvensters en de uitzonderingen worden nader vastgelegd in de SLA. Daarbij wordt de beschikbaarheid gemeten voor de onderdelen waarvoor de opdrachtnemer verantwoordelijk is; de gemeente blijft verantwoordelijk voor de onderdelen binnen haar eigen beheer en contractrelatie.
58	PvE A, eisen 2.20, 4.17 en 8.7 (pp.7,14,22) Bijlage A1 SLA8 (p.4)	Voor de verplichte 24/7-escalatie van P1- en P2-incidenten: beschikt de gemeente vanaf livegang over geautoriseerde, 24/7 bereikbare contactpersonen en vervangers die besluiten over containment kunnen nemen? Welke procedure en verantwoordelijkheidsafbakening gelden wanneer geen contactpersoon bereikbaar is en geen voorafgaand responsmandaat bestaat?	De aanbestedingsstukken schrijven voor dat de opdrachtgever en de opdrachtnemer vóór ingebruikname samen een escalatiematrix vaststellen. Daarin worden de contactpersonen en vervangers, hun bereikbaarheid, verantwoordelijkheden en de criteria voor opschaling opgenomen. De gemeente garandeert in de aanbestedingsstukken echter niet afzonderlijk dat bepaalde medewerkers 24/7 bereikbaar zijn of bevoegd zijn om tijdens een incident besluiten over containment te nemen. De concrete contact- en bereikbaarheidsafspraken worden dus in de escalatiematrix en het DAP uitgewerkt. De SOC-dienstverlening moet kritieke en hoge meldingen 24/7 triëren, analyseren en zo nodig escaleren volgens de overeengekomen termijnen. Als de gemeente niet bereikbaar is en voor een responsactie geen voorafgaand schriftelijk mandaat heeft verleend, mag de opdrachtnemer die actie niet uitvoeren. Responsacties in de gemeentelijke omgeving zijn op grond van eis 4.17 uitsluitend toegestaan binnen vooraf schriftelijk vastgelegde bevoegdheden en mandaten. De opdrachtnemer blijft wel verantwoordelijk voor de vereiste triage, analyse, melding, escalatie en het geven van advies; hij registreert de contactpogingen en het resterende risico en volgt het afgesproken escalatiepad. De gemeente blijft verantwoordelijk voor besluitvorming over bedrijfsimpact en risicoacceptatie en voor niet-gemandateerde responsacties.
59	Bijlage A1, eis DIV31 (p.3); Bijlage G art. 1.3 (pp.36–37); GIBIT art. 22.8 en 27.14 (pp.25,29)	Eis DIV31 schrijft vernietiging van SIEM-logdata en SOC-rapportagedata uiterlijk één jaar na vastlegging voor, terwijl GIBIT artikel 22.8 vernietiging tijdens de overeenkomst zonder verzoek van opdrachtgever beperkt. Geldt DIV31 als vooraf overeengekomen vernietigingsinstructie? Welke bewaartermijnen en uitzonderingen gelden voor incidentdossiers, Sentinel, SOC-systemen en back-ups, mede na afloop van het contract wanneer wettelijke bewaarplichten of technisch noodzakelijke back-upcycli verwijdering nog verhinderen? Kan worden bevestigd dat de vernietigingsverklaring uitsluitend betrekking heeft op gegevens die rechtmatig en feitelijk kunnen worden verwijderd?	De opdrachtgever verduidelijkt dat Bijlage A1, eis DIV31, een vooraf overeengekomen instructie bevat voor de daar omschreven gegevens: logdata binnen de SIEM-oplossing en rapportagedata binnen de SOC-omgeving worden uiterlijk één jaar na vastlegging vernietigd. De opdrachtgever bepaalt vóór ingebruikname de toepasselijke bewaartermijn binnen dat maximum. De vernietiging vindt plaats volgens de vastgelegde bewaartermijn en werkwijze, met inachtneming van de GIBIT en eventuele wettelijke bewaarplichten. De termijn van DIV31 geldt voor de genoemde log- en rapportagedata. Zij stelt niet zonder meer een bewaartermijn vast voor alle incidentdossiers of andere registraties; de bewaartermijn daarvoor wordt bepaald aan de hand van de aard en het doel van de gegevens en schriftelijk met de opdrachtgever vastgelegd. Eventuele wettelijke bewaarplichten en tijdelijke technische beperkingen, zoals het uitfaseren van back-ups volgens een vaste cyclus, moeten vooraf transparant worden gemaakt en mogen niet leiden tot ongeoorloofde verdere verwerking of gebruik van gegevens. Na afloop van de overeenkomst geldt de overeengekomen exit- en verwijderingsprocedure. De vernietigingsverklaring bevestigt de vernietiging van gegevens die volgens de overeenkomst moeten worden vernietigd en die rechtmatig en feitelijk verwijderbaar zijn. Gegevens die wegens een wettelijke bewaarplicht tijdelijk moeten worden bewaard of die nog in een niet direct aanpasbare back-upcyclus aanwezig zijn, worden daarin afzonderlijk verantwoord, afgeschermd van regulier gebruik en verwijderd zodra de bewaarplicht of technische beperking is geëindigd. De opdrachtnemer vermeldt daarbij de resterende gegevens, de reden van bewaring en de uiterste verwijderdatum.

60	PvE A, eis 2.6 (p.5) Verwerkersovereenkomst art.4.3 (p.2)	Eis 2.6 vereist voorafgaande schriftelijke toestemming voor iedere verwerking of opslag buiten de EER, inclusief subverwerkers en supportlocaties. Artikel 4.3 van de verwerkersovereenkomst noemt voorafgaande kennisgeving en AVG-grondslagen. Welke autorisatieplicht geldt bij internationale supporttoegang of incidentele toegang vanaf buiten de EER: voorafgaande schriftelijke toestemming of uitsluitend voorafgaande kennisgeving?	Voor opslag en verwerking van gegevens buiten de EER geldt eis 2.6: dit is uitsluitend toegestaan na voorafgaande schriftelijke instemming van de opdrachtgever. De bepaling ziet uitdrukkelijk ook op subverwerkers, supportlocaties en aanvullende systemen waarin gegevens van de opdrachtgever worden verwerkt. Een voorafgaande kennisgeving alleen is dus niet voldoende. Dit geldt ook voor internationale supporttoegang of incidentele toegang vanaf buiten de EER, voor zover die toegang ertoe leidt dat gegevens van de opdrachtgever vanuit buiten de EER worden geraadpleegd of anderszins beschikbaar worden gesteld. De locatie waar gegevens fysiek zijn opgeslagen is daarbij niet op zichzelf doorslaggevend. Als ondersteuning volledig vanuit de EER plaatsvindt en geen gegevens buiten de EER toegankelijk worden gemaakt, is op grond van eis 2.6 geen afzonderlijke toestemming voor doorgifte buiten de EER vereist. Artikel 4.3 van de verwerkersovereenkomst moet in samenhang met eis 2.6 worden gelezen. De verwerkersovereenkomst en de daarin genoemde AVG-grondslagen vervangen de expliciete eis van voorafgaande schriftelijke instemming niet. De opdrachtnemer moet eventuele betrokkenheid van partijen of supportlocaties buiten de EER vooraf inzichtelijk maken; verwerking of toegang buiten de EER vindt pas plaats na de vereiste schriftelijke instemming en nadat aan de toepasselijke AVG-voorwaarden voor internationale doorgifte is voldaan.
61	PvE A, eis 2.27 (p.8) Verwerkersovereenkomst art.4.5 (p.2) Leidraad §2.2.2 (p.12)	De verwerkersovereenkomst verleent algemene toestemming voor subverwerkers met kennisgeving van wijzigingen; eis 2.27 verlangt voorafgaand akkoord voor delen van gegevens met derden en de leidraad verlangt voorafgaande schriftelijke toestemming voor niet eerder voorgestelde onderaannemers. Welk goedkeuringsproces geldt voor reeds bekende Microsoft- en SOC-subverwerkers en voor wijzigingen gedurende de contractduur?	De opdrachtgever maakt onderscheid tussen de reeds bij inschrijving voorgestelde partijen en eventuele nieuwe partijen die later worden ingeschakeld. Voor zover Microsoft- en SOC-partijen bij inschrijving zijn opgegeven en in de verwerkersovereenkomst of de daarbij behorende lijst zijn opgenomen, geldt de daarin vastgelegde toestemming en kennisgevingsprocedure. Voor nieuwe of gewijzigde subverwerkers geldt de procedure uit de verwerkersovereenkomst: de opdrachtnemer stelt de opdrachtgever vooraf in kennis van de voorgenomen wijziging en geeft de opdrachtgever de daarin overeengekomen gelegenheid om bezwaar te maken. Als voor een partij of gegevensverwerking daarnaast op grond van eis 2.27 voorafgaande accordering is vereist, moet die accordering eveneens vooraf worden verkregen. Los daarvan bepaalt paragraaf 2.2.2 van de aanbestedingsleidraad dat de inzet van een onderaannemer die niet bij de aanbestedingsprocedure is voorgesteld, voorafgaande schriftelijke toestemming van de opdrachtgever vereist. Een kennisgeving op grond van de verwerkersovereenkomst vervangt die toestemming niet. Ook blijven de afzonderlijke eisen voor doorgifte of toegang vanuit buiten de EER gelden: daarvoor is voorafgaande schriftelijke toestemming nodig overeenkomstig eis 2.6. Kortom: een reeds bekendgemaakte en geaccordeerde partij volgt de procedure voor wijzigingen in de verwerkersovereenkomst; een niet eerder voorgestelde onderaannemer vereist voorafgaande schriftelijke toestemming. Elke toepasselijke goedkeurings- of kennisgevingsplicht moet worden nageleefd; de ene procedure heft de andere niet op.
62	Bijlage A1, eisen A28-A32 (p.4) GIBIT art.10.14 en 11.3 (pp.16-17)	Bijlage A1 verlangt dat alle toekomstige wettelijk verplichte modules in de inschrijfprijs zijn inbegrepen en nieuwe wet- en regelgeving tijdig, soms direct en al drie maanden vóór inwerkingtreding, is verwerkt. Hoe wordt omgegaan met tijdens de contractduur nog onbekende of onvoorzienbare wettelijke wijzigingen, die nieuwe functionaliteit of substantiële investering vereisen? Blijft de meerwerkregeling van GIBIT artikel 11.3 hiervoor gelden?	De zinsnede '*Dit moet worden meegenomen in de inschrijfprijs.*' in eis A30 van bijlage A1 vervalt. De meerwerkregeling conform artikel 11.3 van Gibit blijft van toepassing.

63	Bijlage G art. 1.3 (pp.36–37); GIBIT art. 2.5, 3.5 en 21.3 (pp.7–9,23); PvE A eisen 2.6 en 2.27 (pp.5,8)	Artikel 1.3 van bijlage G kent aan het aanbestedingsdocument en bijlagen voorrang boven de GIBIT toe, terwijl GIBIT artikel 2.5 voor derdenprogrammatuur onder voorwaarden toepasselijke licentie- en onderhoudsvoorwaarden laat prevaleren. Welke rangorde geldt bij Microsoft Sentinel en overige SaaS-diensten van derden? Kan worden bevestigd dat opdrachtnemer alleen gebruiksrechten hoeft te verstrekken die de betreffende rechthebbende daadwerkelijk verleent (GIBIT art. 21.3), en dat eventuele uitzonderingen op de expliciete privacy-, dataresidentie- en beveiligingseisen vóór inschrijving kenbaar worden gemaakt?	Artikel 1.3 van de conceptovereenkomst blijft in stand, met dien verstande dat hieraan de volgende verduidelijking wordt toegevoegd: “In afwijking van de in artikel 1.3 van bijlage G opgenomen rangorde geldt voor Derdenprogrammatuur het bepaalde in artikel 2.5 onder i GIBIT 2025, voor zover het de betreffende Derdenprogrammatuur betreft en mits is voldaan aan de informatieverplichtingen van artikel 3.5 GIBIT 2025.” Voor Derdenprogrammatuur gelden derhalve de toepasselijke licentie- en onderhoudsvoorwaarden van de betreffende rechthebbende overeenkomstig het voorgaande. Opdrachtnemer is daarbij niet gehouden gebruiksrechten te verstrekken die de betreffende rechthebbende niet verleent. Dit doet geen afbreuk aan de overige eisen uit de aanbestedingsstukken, waaronder de eisen inzake privacy, dataresidentie en informatiebeveiliging. Eventuele onverenigbaarheden met voorwaarden van derden dienen vóór inschrijving kenbaar te worden gemaakt.
64	Leidraad §6.6 (p.28) Bijlage J, deel I en definitie opdrachtwaarde (pp.2,10)	Voor deze opdracht geldt 2% social return; het uitvoeringsprotocol rekent eventuele verlengingen mee in de totale opdrachtwaarde. Moet de volledige verplichting over de maximale negenjarige contractwaarde al binnen de initiële drie jaar worden gerealiseerd, of wordt zij naar rato van de daadwerkelijk afgenomen contractjaren en gerealiseerde waarde vastgesteld en bij verlenging bijgesteld?	Pas na gunning van de opdracht zal de winnende partij afstemming hebben met hetAdviespunt Social Return over de daadwerkelijke wijze van invulling van Social Return. Naar verwachting is de verplichting gebaseerd op de totale waarde van de opdracht, exclusief btw, inclusief eventuele opties of verlengingen van de overeenkomst (en dus 9 jaar), maar deze dient niet direct volledig in de eerste drie jaar gerealiseerd te worden. Een en ander in afstemming en overleg met Avres.
65	Bijlage G art. 1.2-1.3 (pp.36-37) PvE A, eis 8.1 (p.21) GIBIT art. 2.5 (pp.7-8)	Artikel 1.3 van bijlage G noemt de overeenkomst, de nota's van inlichtingen, het aanbestedingsdocument, de GIBIT en de aanbieding, maar niet afzonderlijk de na gunning vast te stellen SLA, het DAP en de verwerkersovereenkomst. Artikel 2.5 GIBIT kent aan nadere overeenkomsten, waaronder de SLA en verwerkersovereenkomst, juist een hogere rang toe. Welke contractuele positie en rangorde krijgen de definitieve SLA, het DAP en de verwerkersovereenkomst? Kan deze rangorde expliciet en eenduidig in bijlage G worden vastgelegd?	Artikel 1.3 van de conceptovereenkomst blijft (behoudens vraag en antwoord 63) ongewijzigd in stand. De verwerkersovereenkomst wordt als afzonderlijke overeenkomst tussen Partijen gesloten en valt als zodanig niet onder de in artikel 1.3 van de conceptovereenkomst opgenomen rangorde. De SLA en het DAP worden na gunning nader uitgewerkt en vastgesteld binnen de kaders van het Programma van Eisen, de Inschrijving en de Overeenkomst. De SLA en het DAP dienen ter nadere uitwerking van de dienstverlening en kunnen niet worden gebruikt om af te wijken van de in de aanbestedingsstukken en de Inschrijving vastgelegde eisen, voorwaarden en verplichtingen. Een aanpassing van artikel 1.3 van de conceptovereenkomst is derhalve niet noodzakelijk.
66	Bijlage F1, rij 47 (extra use-case) PvE A eisen 2.22, 2.32 en 5.5 (pp.7–9,16)	Welke minimale jaarlijkse inspanning of hoeveelheid aanvullende use-cases, detectieregels, connectoraanpassingen en SOAR-playbooks is in de vaste beheerprijs inbegrepen? Bijlage F1, rij 47, biedt tevens een optioneel tarief voor 'Opnemen extra use case op wens van de klant'. Vanaf welk punt kan een aanvullende use-case separaat worden gefactureerd in plaats van als regulier onderhoud en doorontwikkeling te gelden?	De aanbestedingsstukken schrijven geen minimale jaarlijkse hoeveelheid aanvullende use-cases, detectieregels, connectoraanpassingen of SOAR-playbooks voor boven op de vijf initiële use-cases en de overige overeengekomen dienstverlening. De benodigde werkzaamheden voor het beheren, onderhouden, testen en optimaliseren van de overeengekomen use-cases en detectieregels vallen binnen de vaste dienstverlening, overeenkomstig eisen 2.22 en 2.32 en de inschrijving van de opdrachtnemer. Bijlage F1 vermeldt ‘Opnemen extra use case op wens van de klant’ als een dienst zonder afnameverplichting. Die prijsregel is bedoeld voor een aanvullende use-case die de opdrachtgever afzonderlijk wenst af te nemen; opname van de post verplicht de opdrachtgever niet tot afname. De aanbestedingsstukken leggen echter geen kwantitatieve grens vast waarmee in alle gevallen kan worden bepaald wanneer een activiteit regulier onderhoud is en wanneer sprake is van een afzonderlijke aanvullende use-case. Om die reden kan de opdrachtgever geen vast aantal inbegrepen uitbreidingen of een algemene grens opgeven. De opdrachtnemer moet zijn vaste dienstverlening en de reikwijdte van de optionele prijsregel in de inschrijving duidelijk afbakenen. Een aanvullende use-case wordt alleen afzonderlijk gefactureerd als de opdrachtgever die vooraf afzonderlijk opdraagt en de werkzaamheden aantoonbaar buiten de overeengekomen scope vallen.

67	PvE A, eisen 5.4-5.5 en 5.9 (pp.16-17) Bijlage G art. 3 (p.37) GIBIT art. 11.10 (p.18)	Het PvE verlangt dat alle noodzakelijke kosten in de opgegeven prijzen zijn inbegrepen en staat bij verlenging geen aanvullende toeslagen toe. GIBIT artikel 11.10 biedt echter ruimte voor doorbelasting van onvoorzienbare prijsstijgingen van derdenprogrammatuur; artikel 3 van bijlage G koppelt de vergoeding aan de ingediende prijs. Kan worden bevestigd of artikel 11.10 onverkort geldt voor aantoonbare onvoorzienbare kostenstijgingen van onder meer Microsoft-licenties en cloudcomponenten, en hoe deze worden verwerkt zonder strijd met de vaste prijsafspraken?	De opdrachtgever bevestigt dat artikel 11.10 GIBIT 2025 van toepassing is op aantoonbare prijsstijgingen van Derdenprogrammatuur, voor zover die stijging bij het sluiten van de overeenkomst nog niet voorzienbaar was. Een beroep op dit artikel geldt alleen voor zover de betreffende software onder de GIBIT-definitie van Derdenprogrammatuur valt en de kosten daadwerkelijk aan de gemeente worden doorbelast. Dit betekent niet dat elke prijsstijging van Microsoft-licenties of cloudverbruik automatisch voor vergoeding in aanmerking komt. Zoals eerder verduidelijkt, komen Microsoft Sentinel-, Log Analytics-, Logic Apps- en overige Azure-verbruikskosten die rechtstreeks via de eigen Microsoft-contract- en factureringsrelatie van de gemeente lopen, voor rekening van de gemeente en maken zij geen deel uit van de inschrijfsom van de opdrachtnemer. Artikel 11.10 is daarop niet van toepassing, omdat de opdrachtnemer die kosten niet aan de gemeente doorbelast. Eventuele Microsoft-licenties of Derdenprogrammatuur die de opdrachtnemer zelf aan de gemeente levert en factureert, worden beoordeeld aan de hand van artikel 11.10 en de overige contractuele prijsafspraken. De vaste prijsafspraken, de regels over indexering en het verbod op aanvullende kosten blijven onverkort gelden voor de eigen dienstverlening en kosten van de opdrachtnemer. Eventuele doorbelasting op grond van artikel 11.10 moet aantoonbaar zijn en mag niet leiden tot dubbele vergoeding of een aanvullende toeslag voor kosten die al in de inschrijfprijs zijn inbegrepen.
68	Bijlage A1, eis SLA8 (p.4) PvE A, eisen 2.20, 4.2 en 8.5 (pp.7,12,21)	Voor prioriteit 3 en 4 vermeldt SLA8 een reactietijd en escalatietijd van minder dan vier uur, respectievelijk minder dan 8 uur, terwijl de 24/7-plicht in het PvE expliciet op kritieke en hoge meldingen is gericht. Geldt de norm voor P3/P4 ook buiten werkdagen en kantoortijden of uitsluitend binnen het overeengekomen reguliere servicevenster?	De tijden voor Prio 3 en Prio 4 in SLA8 gelden als overeengekomen doorlooptijden voor die prioriteiten; SLA8 zelf beperkt deze tijden niet tot kantooruren. Tegelijk bepaalt eis 2.20 dat de expliciete 24/7-verplichting voor triage, analyse en zo nodig escalatie betrekking heeft op kritieke en hoge meldingen (Prio 1 en 2). Voor Prio 3 en 4 zijn de reactietijd en escalatietijd daarom van toepassing binnen het reguliere servicevenster van de dienstverlening, zoals vast te leggen in de SLA. Detectie en ontvangst van meldingen worden ondersteund door de overeengekomen monitoringvoorziening. De SLA legt per prioriteit het servicevenster, de start- en eindmomenten van de termijnen en de wijze van meten vast. Voor Prio 1 en 2 geldt onverkort de 24/7-afhandeling en escalatie.
69	PvE A, eis 8.6, laatste alinea (p.21) eis 2.2 (p.4)	Eis 8.6 verlangt detectie en melding van uitval van kritieke logstromen binnen één uur. Welke van de vermelde bronnen zijn “kritiek”, wanneer is sprake van uitval (geen events, vertraagde ontvangst of foutmelding) en welke bronafhankelijke polling- of ingestie-intervallen worden bij de meting gehanteerd?	Alle logbronnen gelden als kritiek. Onder uitval wordt verstaan dat een overeengekomen logstroom niet beschikbaar is, onvolledig is of niet binnen de afgesproken bronafhankelijke termijn in Microsoft Sentinel beschikbaar komt. Een enkele periode zonder nieuwe events is op zichzelf niet voldoende om uitval vast te stellen; de beoordeling houdt rekening met de aard van de bron en het verwachte aanlever- of pollingpatroon. De opdrachtnemer monitort de beschikbaarheid, volledigheid en actualiteit van de aangesloten logbronnen en detecteert, registreert en meldt uitval van logstromen binnen één uur, conform eis 8.6. De bronafhankelijke aanlever- en pollingintervallen en de methode om uitval te signaleren worden tijdens de implementatie vastgesteld en in de SLA en het DAP opgenomen. Daarbij wordt onderscheid gemaakt tussen de detectie van problemen met de logbron of connector en de verwerkingstijd van data door Microsoft Sentinel; de meetwijze voor die verwerkingstijd sluit aan bij het antwoord op vraag 25 in de Nota van Inlichtingen.
70	Leidraad §2.2.1 en §6.3 (pp.12,27); PvE A eis 4.1 (p.12); GIBIT art. 15.2 (p.21)	De leidraad schrijft Nederlandse communicatie en Nederlandstalige inschrijvingsdocumenten voor. Eis 4.1 staat operationele communicatie in het Engels na toestemming toe, terwijl GIBIT artikel 15.2 Engelstalige overige (niet-eindgebruikers-)documentatie toestaat. Kan de gemeente bevestigen dat bestaande technische documentatie, handleidingen van Microsoft/derden en specialistische operationele informatie in het Engels mogen worden aangeleverd wanneer geen Nederlandse versie beschikbaar is, mits formele rapportages, adviezen en incidentmeldingen voor de gemeente in het Nederlands worden verzorgd? Geldt een vergelijkbare uitzondering voor specialistische technische escalaties?	Ja, bestaande technische documentatie van Microsoft en andere derden, en specialistische operationele informatie, mogen in het Engels worden verstrekt als daarvan geen Nederlandse versie beschikbaar is. Dit betreft niet-eindgebruikersdocumentatie en sluit aan bij GIBIT 2025, artikel 15.2, dat overige documentatie in het Engels toestaat. Formele rapportages, adviezen en incidentmeldingen die voor de gemeente zijn bestemd, worden in het Nederlands verzorgd, overeenkomstig de aanbestedingsleidraad en eis 4.1 van het Programma van Eisen. Specialistische operationele communicatie en technische escalaties mogen, na instemming van de opdrachtgever, in het Engels plaatsvinden wanneer dat voor de benodigde technische ondersteuning noodzakelijk is.

71	PvE A, eis 3.4 (p.10) Verwerkersovereenkomst art.4.2 (p.2) GIBIT art.28.8	Eis 3.4 verplicht opdrachtnemer jaarlijks kosteloos medewerking te verlenen aan maximaal twee reguliere audits, terwijl artikel 4.2 van de verwerkersovereenkomst en GIBIT artikel 28.8 in beginsel kosten bij opdrachtgever leggen. Welke regeling geldt voor reguliere privacy-, beveiligings- en wettelijke audits, en welke auditinzet moet in de vaste prijs worden inbegrepen?	De opdrachtnemer verleent per contractjaar kosteloos medewerking aan maximaal twee audits, zoals bepaald in eis 3.4.
72	Bijlage A1, eis A34 (p.4); PvE A eisen 2.23 en 6.3 (pp.8,18); GIBIT art. 21.1 en 21.4 (p.23)	Eis A34 ziet noodzakelijk maatwerk als onderdeel van de standaard ICT-prestatie, terwijl het PvE en de GIBIT onderscheid maken tussen klantspecifieke resultaten en al bestaande intellectuele eigendomsrechten. Kan worden bevestigd dat overdracht van rechten uitsluitend ziet op voor opdrachtgever specifiek ontwikkelde maatwerkprogrammatuur en dat bestaande generieke SOC-content, detectieregels, playbooks, connectorbibliotheken, templates, frameworks, methodieken en knowhow eigendom van opdrachtnemer of derden blijven, met voor de gemeente toereikende gebruiks- en overdrachtsrechten?	Eis A34 bepaalt dat noodzakelijk maatwerk onderdeel wordt van de standaard aangeboden ICT-prestatie. In samenhang met eisen 2.23 en 6.3 bevestigt de opdrachtgever dat dit niet betekent dat reeds bestaande generieke SOC-content, detectieregels, playbooks, connectorbibliotheken, templates, frameworks, methodieken of knowhow eigendom van de gemeente worden. Deze generieke componenten blijven eigendom van de opdrachtnemer of de betreffende derde, ook wanneer zij in de gemeentelijke tenant worden gebruikt. Voor die generieke componenten krijgt de gemeente het in eis 2.23 genoemde gebruiksrecht, toereikend voor de uitvoering, continuïteit en overdracht van de dienstverlening. Klantspecifieke resultaten en configuraties die specifiek voor de gemeente worden ontwikkeld of gerealiseerd, vallen onder de eigendomsregeling van eisen 2.23 en 6.3. Welke rechten precies gelden, volgt uit de aard van het betreffende onderdeel en de afspraken in de overeenkomst. De GIBIT 2025 bepaalt als uitgangspunt dat intellectuele-eigendomsrechten op de door de leverancier ter beschikking gestelde ICT-prestatie bij de leverancier of diens licentiegevers berusten, tenzij anders is overeengekomen. De kwalificatie als Maatwerkprogrammatuur wordt bepaald aan de hand van de GIBIT-definitie en de concrete ontwikkeling. Voor zover een onderdeel specifiek voor de opdrachtgever, in diens schriftelijke opdracht en voor diens kosten wordt ontwikkeld, gelden de toepasselijke GIBIT-bepalingen voor maatwerkprogrammatuur; de algemene benaming “onderdeel van de standaard ICT-prestatie” wijzigt die kwalificatie op zichzelf niet.
73	Bijlage A1, eis TECH25 (p.3) PvE A, eisen 2.7 en 2.25 (pp.5,8)	Bijlage A1 vereist een app op Android, iPhone of iPad. Is een via de mobiele browser beveiligd en volledig bruikbaar Microsoft Sentinel- of SOC-portaal (met MFA) voldoende, of wordt een afzonderlijk installeerbare native app als uitsluitende eis verlangd? Welke concrete mobiele functies moeten minimaal beschikbaar zijn?	TECH25 komt te vervallen, zoals beschreven in vraag en antwoord 37
74	Bijlage A1, eis TECH57 (p.5) Leidraad §1.1.1 (p.5)	Eis TECH57 verlangt ondersteuning van alle door Microsoft ondersteunde Windows-versies en M365-apps. Op welke onderdelen van de feitelijk te leveren SIEM/SOC-dienst ziet deze eis: uitsluitend de ondersteunde endpoint-/logconnectoren en beheertoegang, of ook functionaliteit van alle gemeentelijke besturingssystemen en applicaties waarop opdrachtnemer geen invloed heeft?	TECH57 geldt voor de compatibiliteit van de door de opdrachtnemer geleverde of beheerde SIEM/SOC-dienstverlening met de door Microsoft ondersteunde Windows-versies en Microsoft 365-apps. Voor zover een logbron of endpoint-agent nodig is voor de overeengekomen monitoring, moet de gebruikte connector of agent de relevante, ondersteunde Windows-omgeving kunnen ondersteunen. TECH57 betekent niet dat de opdrachtnemer verantwoordelijk wordt voor de werking, beschikbaarheid of ondersteuning van alle gemeentelijke besturingssystemen en applicaties waarop hij geen invloed of beheerbevoegdheid heeft. De gemeente blijft verantwoordelijk voor haar eigen bron- en doelsystemen; de opdrachtnemer is verantwoordelijk voor de aansluiting en verwerking van de overeengekomen beveiligingsgegevens binnen de grenzen van de opdracht. De precieze ondersteunde systemen, connectoren en afhankelijkheden worden vastgelegd in het ontwerp en het DAP.

75	PvE A, eisen 2.16, 2.19, 2.21, 2.23 en 4.7, 4.19 (pp. 7, 12, 15)	De genoemde bepalingen schrijven Microsoft Sentinel binnen de gemeentelijke tenant voor als centraal incidentregistratieplatform en verbieden een zelfstandige SIEM-omgeving buiten de tenant. Kan de Aanbestedende Dienst bevestigen dat een hybride architectuur is toegestaan waarbij Microsoft Sentinel het primaire platform voor gemeentelijke logdata blijft, en relevante detecties, incidentgegevens en noodzakelijke context via beveiligde koppelingen worden verwerkt in centrale analyse-, correlatie-, SOAR- en incidentafhandelingstooling op het platform van Opdrachtnemer, mits de gemeentelijke zeggenschap, rechtstreekse toegang en gegevensbescherming binnen de EER gewaarborgd blijven? Kan tevens expliciet worden confirmed dat deze ondersteunende, centrale SOC-tooling van Opdrachtnemer niet wordt aangemerkt als een verboden zelfstandige SIEM-omgeving buiten de tenant? Kan de gemeente daarbij tevens bevestigen dat noodzakelijke incidentmetadata, gecategoriseerde alarmtitels, detectieregels en onderzoekscontext in dit ondersteunende centrale SOC-platform binnen de EER mogen worden verwerkt, terwijl de ruwe gemeentelijke loggegevens en de Microsoft Sentinel-omgeving onder de zeggenschap van de gemeente blijven?	De aanbestedende dienst bevestigt dat Microsoft Sentinel binnen de Microsoft-tenant van de gemeente het primaire platform blijft voor gemeentelijke logdata, beveiligingsmeldingen en incidentregistratie. Een ondersteunende centrale SOC-omgeving van de opdrachtnemer mag daarnaast worden gebruikt voor analyse, correlatie, SOAR en incidentafhandeling, mits de gemeentelijke zeggenschap en rechtstreekse toegang tot Sentinel behouden blijven en aan de eisen voor beveiliging, gegevensbescherming en gegevenslocatie wordt voldaan. Het verbod op een zelfstandige SIEM-omgeving buiten de tenant ziet op het vervangen van Sentinel door een afzonderlijke SIEM-omgeving van de opdrachtnemer als primair platform voor de gemeentelijke logdata en incidentregistratie. Het verbiedt niet het gebruik van ondersteunende SOC-tooling, zolang die niet als zelfstandige vervangende SIEM-omgeving wordt ingezet. Noodzakelijke incidentmetadata, gecategoriseerde alarmtitels en onderzoekscontext mogen, voor zover noodzakelijk voor de dienstverlening, via beveiligde koppelingen in die ondersteunende omgeving worden verwerkt binnen de EER. Ruwe gemeentelijke logdata en de Sentinel-omgeving blijven onder de zeggenschap van de gemeente. De opdrachtnemer documenteert welke gegevens naar de ondersteunende SOC-tooling worden overgebracht, met welk doel, waar deze worden verwerkt en hoe lang zij worden bewaard. Gebruik van klantspecifieke detectieregels of configuraties en overdracht daarvan blijven onderworpen aan de rechten van de gemeente zoals beschreven in eisen 2.23 en 6.3. De aanbestedingsstukken verlangen daarnaast dat geautoriseerde gemeentelijke medewerkers rechtstreeks toegang houden tot Sentinel en tot relevante loggegevens, meldingen, incidenten en onderzoeksgegevens. De ondersteunende SOC-tooling mag deze toegang of zeggenschap niet beperken.
76	Leidraad §5.1.1 (p.24)	Voor de uitwerking van A, B en C zijn gezamenlijk maximaal acht A4-pagina’s beschikbaar. Tellen omslag, inhoudsopgave, afbeeldingen, planning, het bij gunningscriterium B verlangde RACI-model en eventuele bewijsbijlagen mee in deze acht pagina’s?	Ja dit zijn inderdaad 8 inhoudelijke pagina's en het is dus akkoord dat dit exclusief voorblad/omslag, inhoudsopgave en eventuele bijlage(s) is. Als bijlagen buiten de acht inhoudelijke A4 mogen uitsluitend de planning en het RACI-model worden toegevoegd. Afbeeldingen vallen dus wel (ook) onder het maximale van acht (8) pagina's A4.
77	Leidraad §5.1.1, criterium D (pp.23-24)	Is het toegestaan de demonstratie uit te voeren in een representatieve eigen Microsoft Sentinel-demo-omgeving met gesimuleerde en geanonimiseerde incidenten, mits de getoonde configuraties en SOC-processen overeenkomen met het aangeboden productieservicemodel? Worden eventuele aanvullende scenario’s vooraf gelijkelijk aan alle inschrijvers bekendgemaakt?	Ja. De demonstratie mag worden uitgevoerd in een representatieve eigen Microsoft Sentinel-demo-omgeving, met gesimuleerde en geanonimiseerde incidenten. De getoonde configuraties, functionaliteiten en SOC-processen moeten overeenkomen met de aangeboden oplossing en het servicemodel dat de inschrijver bij gunning zal leveren. De demonstratie dient ter verificatie van de inschrijving en mag niet worden gebruikt om deze inhoudelijk te wijzigen of aan te vullen. De aanbestedingsstukken voorzien in een use-case naar keuze en in vragen of aanvullende scenario’s tijdens de demonstratie. Als de gemeente aanvullende scenario’s vooraf vaststelt, worden deze tijdig en op gelijke wijze aan alle inschrijvers bekendgemaakt. Tijdens de demonstratie kunnen daarnaast vragen of scenario’s worden voorgelegd die aansluiten bij de beschreven beoordelingsaspecten.
78	Leidraad §5.1.1, criterium D (p.24) §5.2 (pp.25-26)	Paragraaf 5.2 beschrijft de rapportcijferbeoordeling expliciet voor A, B en C, terwijl bijlage D ook voor de demonstratie (D) een cijfer en fictieve meerwaarde gebruikt. Kan worden bevestigd dat criterium D volgens dezelfde cijferschaal en meerwaardestappen wordt beoordeeld, en hoe de specifieke demonstratieaspecten in één eindcijfer worden gewogen?	Voor zover in paragraaf 5.2 uitsluitend wordt verwezen naar de gunningscriteria A, B en C, dient dit voor de toepassing van de cijferschaal en de fictieve meerwaardesystematiek te worden gelezen als A, B, C en D. Voor het overige blijven de aanbestedingsstukken ongewijzigd. De bij gunningscriterium D genoemde beoordelingsaspecten worden integraal en in onderlinge samenhang beoordeeld en leiden tot één eindcijfer. Aan de afzonderlijke beoordelingsaspecten wordt geen afzonderlijke weging of deelscore toegekend.

79	PvE A, eisen 5.8 en 7.7 (pp.17,20) Bijlage A1, eis SLA1.3 (p.4) GIBIT art.29.4	Het PvE rekent reguliere exit- en re-transitiewerkzaamheden tot de vaste prijs en bijlage A1 schrijft een gezamenlijke test van het exitplan voor. Welke omvang, frequentie en ureninzet van deze test zijn inbegrepen en geldt voor additionele migratieactiviteiten buiten die vaste scope de meerwerkregeling, ondanks de generieke vergoedingsbepaling van GIBIT artikel 29.4?	Het opstellen, actueel houden en regulier uitvoeren van het Exitplan, waaronder de daarin opgenomen gezamenlijke test, is inbegrepen in de aangeboden prijs. De aanbestedingsstukken schrijven geen vaste testfrequentie, testduur of ureninzet voor. De omvang en planning van de gezamenlijke test worden in het Exitplan uitgewerkt en afgestemd. Inschrijvers dienen hiervoor in hun prijs rekening te houden met een passende, uitvoerbare test van het plan gedurende de contractperiode. De vaste prijs omvat de reguliere exit- en re-transitiewerkzaamheden zoals omschreven in eisen 5.8 en 7.7. Werkzaamheden die aantoonbaar buiten de overeengekomen exitverplichtingen vallen, kunnen alleen als meerwerk worden uitgevoerd na voorafgaande schriftelijke opdracht van de opdrachtgever. Dit moet worden gelezen in samenhang met de GIBIT: de algemene vergoedingsbepaling laat de specifieke prijsafspraken in de aanbestedingsstukken onverlet. De opdrachtgever bevestigt daarom niet dat alle mogelijke aanvullende migratieactiviteiten zonder onderscheid in de vaste prijs zijn inbegrepen, noch dat zij automatisch als meerwerk gelden; beslissend is of de werkzaamheden binnen de overeengekomen reguliere exit-scope vallen.
80	Bijlage A1, eis SLA8 (p.4) PvE A, eis 4.7 (p.12)	SLA8 verlangt escalatie via een geautomatiseerd platform dat telefonie, pushberichten, sms en e-mail ondersteunt; eis 4.7 noemt e-mail/telefoon en een toegankelijk portaal. Zijn al deze kanalen bij elk afzonderlijk P1/P2-incident verplicht parallel te gebruiken, of volstaat aantoonbare telefonische escalatie met geautomatiseerde fallback en registratie in het portaal?	Nee, de aanbestedingsstukken vereisen niet dat bij ieder P1- of P2-incident alle genoemde kanalen gelijktijdig worden gebruikt. SLA8 vereist een geautomatiseerd escalatieplatform dat voor het 24/7 escaleren van P1- en P2-incidenten meerdere communicatiekanalen ondersteunt: telefonie, pushnotificaties, sms en e-mail. Ook moet het platform escalatie naar vervangende contactpersonen ondersteunen als er geen reactie komt. De gekozen escalatieprocedure en inzet van de kanalen per prioriteit en situatie worden vastgelegd in de escalatiematrix, de SLA en het DAP. Voor P1 en P2 geldt dat de melding telefonisch wordt geëscaleerd. De overige beschikbare kanalen kunnen worden ingezet voor aanvullende notificatie of als fallback volgens de overeengekomen procedure. Het incident wordt daarnaast geregistreerd in het voor de gemeente toegankelijke portaal, overeenkomstig eis 4.7.
81	Bijlage F1, rij 49 (optionele 'eyes on screen') PvE A eisen 2.20, 4.2 en 8.5 (pp.7,12,21)	Bijlage F1 noemt '24x7x365 eyes on screen meerprijs t.o.v. piket-dienst' als dienstverlening zonder afnameverplichting. Het PvE verlangt echter 24/7 detectie, ontvangst en verwerking van meldingen en 24/7 triage en escalatie bij P1/P2. Welk operationeel bezettings- en bewakingsniveau moet in de verplichte basisprijs zijn inbegrepen? Is een combinatie van geautomatiseerde bewaking en 24/7 bereikbare piketanalisten toegestaan mits alle SLA-normen worden gehaald, en waarin verschilt de optionele 'eyes on screen'-dienst dan precies?	De basisprijs moet voldoen aan de verplichte eisen voor 24/7-dienstverlening. Dat betekent dat beveiligingsmeldingen 24 uur per dag en 7 dagen per week worden gedetecteerd, ontvangen en verwerkt. Kritieke en hoge meldingen (P1 en P2) moeten 24/7 binnen de overeengekomen termijnen worden getrieerd, geanalyseerd en zo nodig geëscaleerd. Eis 2.20 staat toe dat de opdrachtnemer hiervoor een combinatie van automatisering en menselijke analyse inzet. Een 24/7-bereikbare piketdienst is dus toegestaan, mits deze inrichting aantoonbaar alle vereiste kwaliteit, bereikbaarheid en SLA-termijnen haalt. De optionele post ‘24x7x365 eyes on screen meerprijs t.o.v. piket-dienst’ in Bijlage F1 is een aanvullende dienst zonder afnameverplichting. Deze post betreft permanent bemande bewaking van het scherm door analisten, boven op de verplichte basisdienst. De inschrijver beschrijft in zijn aanbieding het verschil tussen de basisdienst en deze optie, waaronder de bezetting en de wijze van opvolging. De optie neemt geen verplichte basisnormen weg en is alleen van toepassing als de gemeente haar afzonderlijk afneemt.
82	Bijlage F1, rijen 13–40 (jaarlijkse logbronkosten) Rijen 35–36 ('overig, namelijk') PvE A eisen 2.20, 5.5 en 5.9 (pp.7,16–17)	Het prijzenblad bevat voor de initiële scope uitsluitend jaarlijkse kosten per logbron en geen afzonderlijke regel voor een vaste SOC-basisdienst, Sentinel-beheer, rapportages, beschikbaarheid en structurele dienstverlening. Verwacht de gemeente dat alle vaste terugkerende SOC-kosten in de logbrontarieven zijn verwerkt, of mogen inschrijvers deze transparant onder 'overig, namelijk' (rijen 35 en 36) opnemen met een aantal van één? Welke wijze van offreren is vereist om verschillende prijsmodellen op gelijke grondslag te vergelijken?	De vaste terugkerende kosten voor de verplichte SOC-dienstverlening moeten in de inschrijfprijs zijn opgenomen. Dit betreft alle kosten die nodig zijn om aan de eisen van het Programma van Eisen te voldoen, waaronder 24/7 monitoring, triage, analyse, escalatie, beheer, rapportages en structurele dienstverlening. De inschrijver vult het prijzenblad volledig in. Als een vaste SOC-basisdienst niet passend kan worden toegerekend aan afzonderlijke logbronnen, mag deze transparant worden opgenomen onder ‘overig, namelijk’ in rij 35 of 36, met een passende omschrijving en eenheid. De inschrijver vult daarbij het aantal en de prijs per eenheid in; een aantal van één kan worden gehanteerd als dat aansluit bij het prijsmodel. De prijs moet tevens worden verwerkt in de jaarlijkse kosten en het subtotaal volgens de formules in het prijzenblad. De opdrachtgever past het prijzenblad niet aan. Om de inschrijvingen vergelijkbaar te maken, moeten inschrijvers alle voor de verplichte dienstverlening noodzakelijke kosten opnemen, eventuele aannames expliciet toelichten en voorkomen dat dezelfde kosten zowel in logbrontarieven als onder ‘overig’ worden meegerekend. Kosten die rechtstreeks door Microsoft aan de gemeente worden gefactureerd, zoals Azure-verbruikskosten, vallen hier niet onder; daarop is de eerdere beantwoording over de Microsoft-kosten van toepassing.

83	Bijlage F1, rijen 28–34, kolommen B–F Bijlage F1, rijen 14–27	In het prijzenblad zijn de regels 28 tot en met 34 als 'per jaar/asset' aangemerkt, maar de omschrijving van de betreffende logbron of asset in kolom B ontbreekt. De omschrijvingscellen lijken bovendien niet als invulvelden beschikbaar onder de bladbeveiliging. Waarvoor zijn deze zeven regels bedoeld: verplichte additionele bronnen, vrij in te vullen bronnen of niet-gebruikte placeholders? Kunt u de omschrijvingen en invulmogelijkheden corrigeren of verduidelijken welke regels inschrijvers leeg moeten laten?	Het prijzenblad is aangepast, zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.
84	Bijlage F1, rijen 43–51 ('scope zonder afnameverplichting') Bijlage F1, cel F40 PvE A eisen 5.2, 5.5 en 5.9 (pp.16–17)	De kosten voor honeypots/deception, additionele use-cases, CERT/IR-retainers en 24/7 'eyes on screen' worden in F51 opgeteld, maar niet betrokken bij de beoordelingsprijs F40. Kunt u bevestigen dat alle posten 46 tot en met 49 uitsluitend facultatief zijn, dat alle daarbij ingevulde eenheidstarieven na gunning wel bindend zijn en dat deze posten niet meewegen in de gunning? Welke uniforme eenheden en rekenaantallen moeten bij deze posten worden ingevuld, zodat optionele tarieven onderling vergelijkbaar zijn?	In het prijzenblad staat dat deze posten optioneel zijn. Deze wegen niet mee in de aanbestedingswaarden. Zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.
85	Bijlage F1, kolommen C–E, rijen 14–27 PvE A eisen 2.2 en 5.5 (pp.4,16)	De prijsregels voor de veertien initiële logbronnen hanteren overal de generieke aanduiding 'per jaar/eenheid', zonder de eenheid per logbron te definiëren. Kan de gemeente per bron specificeren of met 'eenheid' bijvoorbeeld een tenant, gebruiker, beheerd account, endpoint, server, netwerkcomponent, asset of gegevensvolume wordt bedoeld, en op welke wijze dubbeltelling van dezelfde gebruiker of hetzelfde apparaat over meerdere logbronnen moet worden voorkomen?	Het prijzenblad is aangepast, zie bijlage 1 (Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx) bij deze Nota van Inlichtingen.
86	Bijlage G art. 2.2 (p.37)	Artikel 2.2 van de conceptovereenkomst geeft opdrachtgever eenzijdig het recht de overeenkomst driemaal met twee jaar te verlengen, zonder een uiterste aankondigingstermijn te noemen. Bent u bereid op te nemen dat opdrachtgever een eventuele verlenging uiterlijk zes maanden vóór afloop van de dan geldende contractperiode schriftelijk aan opdrachtnemer bekendmaakt?	Nee. De Aanbestedende dienst neemt de voorgestelde aankondigingstermijn niet over. Artikel 2.2 van de conceptovereenkomst blijft ongewijzigd van toepassing. Opdrachtgever behoudt het recht de Overeenkomst overeenkomstig het bepaalde in artikel 2.2 te verlengen. Een vaste uiterste termijn voor het bekendmaken van een besluit tot verlenging wordt niet opgenomen.
87	Bijlage J, deel V (p.8); Leidraad §6.6 (p.28).	Het uitvoeringsprotocol Social Return bepaalt dat een niet-ingevuld deel van de socialreturnverplichting bij de eindafrekening wordt ingehouden dan wel opeisbaar wordt, zonder onderscheid tussen verwijtbare en niet-verwijtbare omstandigheden. Bent u bereid expliciet te bepalen dat deze financiële consequentie uitsluitend geldt bij een aan opdrachtnemer toerekenbare tekortkoming, nadat deze een redelijke gelegenheid heeft gehad alsnog passende invulling te geven aan de verplichting?	Nee. De verantwoordelijkheid voor het realiseren van de Social Return-verplichting blijft bij Opdrachtnemer. Indien de beoogde invulling niet of niet volledig kan worden gerealiseerd, dient Opdrachtnemer tijdig in overleg te treden met het Adviespunt Social Return over een passende alternatieve invulling. Voordat de financiële consequentie wegens het niet (volledig) realiseren van de verplichting wordt toegepast, wordt Opdrachtnemer overeenkomstig het Uitvoeringsprotocol in de gelegenheid gesteld de openstaande verplichting alsnog passend in te vullen. Het Uitvoeringsprotocol blijft ongewijzigd van toepassing.
88	GIBIT 2025 art. 3.2–3.3 (p.8); Leidraad §1.1.1 (pp.5–6); PvE A eis 3.5 (pp.10–11)	GIBIT artikel 3.2 verlangt dat inschrijver zich vooraf voldoende op de hoogte stelt van het gemeentelijke applicatielandschap. Kan de gemeente bevestigen dat alle bij haar bekende, voor een verantwoorde SIEM/SOC-inrichting relevante gegevens over architectuur, tenant, logbronnen, beheergrenzen, bestaande licenties en derde leveranciers volledig en actueel ter beschikking zijn gesteld, of alsnog een overzicht met ontbrekende gegevens en bekende afhankelijkheden verstrekken?	De relevante applicaties zijn genoemd in de 2.2 PVE opgenomen log-bronnen-lijst.

89	GIBIT 2025 art. 4.1–4.3, 17.2 en 27.9 (pp.9,21,29); PvE A eis 3.3 (p.10)	GIBIT artikelen 4.2 en 4.3 kwalificeren bepaalde implementatie- en wettelijke termijnen als fataal. Is de gemeente bereid te bepalen dat opdrachtnemer bij een overschrijding van een dergelijke termijn eerst schriftelijk in gebreke wordt gesteld en een redelijke hersteltermijn krijgt voordat verzuim intreedt, behoudens gevallen waarin nakoming blijvend onmogelijk is?	Nee. De Aanbestedende dienst neemt de voorgestelde wijziging niet over. De artikelen 4.2 en 4.3 GIBIT 2025 blijven ongewijzigd van toepassing. Voor de daarin als fataal aangemerkte termijnen is derhalve geen voorafgaande ingebrekestelling of aanvullende hersteltermijn vereist. Voor zover sprake is van omstandigheden die op grond van de GIBIT van invloed zijn op het fatale karakter van de betreffende termijn of op het intreden van verzuim, gelden de desbetreffende bepalingen van de GIBIT onverkort.
90	GIBIT 2025 art. 6.2 en 6.5 (pp.10–11); Leidraad §1.1 (p.5); PvE A eisen 3.3 en 3.5 (pp.10–11)	GIBIT artikel 6.2 rekent conversie en migratie in beginsel tot de implementatie. Volgens de leidraad beschikt de gemeente echter nog niet over een geïntegreerde SIEM/SOC-oplossing. Kan worden bevestigd dat geen conversie of historische logmigratie vanuit een bestaand SIEM tot de vaste implementatiescope behoort en dat de opdracht zich beperkt tot inrichting van Sentinel, bronontsluiting en de overeengekomen initiële use-cases, tenzij aanvullende migratieactiviteiten afzonderlijk worden opgedragen?	De aanbestedende dienst beschikt momenteel inderdaad niet over een geïntegreerde SIEM/SOC-oplossing. Conversie of migratie van historische loggegevens vanuit een bestaand SIEM maakt daarom geen onderdeel uit van de initiële implementatiescope. De initiële implementatie omvat de in de aanbestedingsstukken beschreven werkzaamheden, waaronder de inrichting van Microsoft Sentinel, het aansluiten van de overeengekomen logbronnen en het implementeren, testen en documenteren van de vijf initiële use-cases. Voor zover voor de uitvoering van deze werkzaamheden gegevensoverdracht, configuratie of koppelingen noodzakelijk zijn, maken deze werkzaamheden wel onderdeel uit van de implementatie. Eventuele aanvullende conversie- of migratiewerkzaamheden die niet uit de in de aanbestedingsstukken beschreven implementatiescope voortvloeien, maken geen onderdeel uit van de vaste implementatiescope en kunnen, indien gewenst, afzonderlijk worden overeengekomen. Artikel 6 GIBIT 2025 blijft voor het overige ongewijzigd van toepassing.
91	GIBIT 2025 art. 9.1 en 9.11 (pp.13–14); PvE A eis 3.3 (p.10)	GIBIT artikel 9.1 regelt acceptatie bij gebreken en artikel 9.11 sluit onthouding van acceptatie bij niet-productieverstorende gebreken uit. Kan de gemeente bevestigen dat acceptatie uitsluitend wordt beoordeeld aan de hand van vooraf schriftelijk vastgestelde en uitdrukkelijk overeengekomen specificaties en dat geringe tekortkomingen die de feitelijke productiegang niet verhinderen geen grond vormen voor het onthouden van acceptatie, mits herstelafspraken worden vastgelegd?	Dit kan worden bevestigd, met dien verstande dat de acceptatie plaatsvindt overeenkomstig artikel 9 GIBIT 2025 en wordt beoordeeld aan de hand van het Overeengekomen gebruik en de daarop van toepassing zijnde eisen en specificaties uit de aanbestedingsstukken, de Overeenkomst en het Implementatieplan. Overeenkomstig artikel 9.11 GIBIT 2025 vormen Gebreken die, afzonderlijk noch gezamenlijk, in de weg staan aan het gebruik voor productieve doeleinden van de betreffende ICT Prestatie geen grond voor het onthouden van Acceptatie. De verplichting van Opdrachtnemer om dergelijke Gebreken op korte termijn te herstellen blijft onverkort van toepassing. De herstelafspraken worden schriftelijk vastgelegd. Artikel 9 GIBIT 2025 blijft ongewijzigd van toepassing.
92	GIBIT 2025 art. 10.16 en 37.4 (pp.16,36); PvE A eisen 8.2–8.3 (p.21)	GIBIT artikel 10.16 biedt opdrachtgever onder voorwaarden ruimte updates of upgrades te weigeren, maar Microsoft Sentinel en andere SaaS-componenten worden door de betreffende platformleverancier centraal doorontwikkeld. Kan worden bevestigd dat opdrachtnemer niet verantwoordelijk wordt gehouden voor het beschikbaar blijven van door Microsoft uitgefaseerde versies of functies en dat voor automatisch doorgevoerde cloudwijzigingen de voor generieke dienstverlening op afstand geldende regeling van artikel 37.4 leidend is?	Aanbestedende dienst kan dit gedeeltelijk bevestigen. Voor generieke Dienstverlening op Afstand is artikel 37 GIBIT 2025 van toepassing. Dit betekent onder meer dat overeenkomstig artikel 37.4 het bepaalde in artikel 10.16 niet van toepassing is op generieke Dienstverlening op Afstand die aan meerdere klanten wordt aangeboden, tenzij anders overeengekomen. De Aanbestedende dienst bevestigt echter niet dat Opdrachtnemer zonder meer wordt ontslagen van zijn verplichtingen indien Microsoft of een andere derde bepaalde versies of functionaliteiten wijzigt of uitfaseert. In dat geval blijven de toepasselijke bepalingen van de GIBIT 2025 en de eisen uit de aanbestedingsstukken ten aanzien van de overeengekomen dienstverlening, onderhoud, continuïteit en Derdenprogrammatuur onverkort van toepassing. De GIBIT 2025 blijft op dit punt ongewijzigd van toepassing.
93	GIBIT 2025 art. 11.2 (p.17); Bijlage G art. 3 (p.37); PvE A eisen 5.6–5.7 (p.17)	GIBIT artikel 11.2 bepaalt dat 30% van eenmalige en periodieke vergoedingen pas opeisbaar wordt na integrale acceptatie. Welke concrete facturatie- en betaalmomenten zijn bedoeld voor de implementatievergoeding, maandelijks doorlopende SOC-diensten en eventueel vooruit te betalen derdenlicenties? Is de gemeente bereid te bevestigen dat de uitgestelde 30% niet wordt toegepast op reeds daadwerkelijk geleverde en geaccepteerde periodieke dienstverlening of op volledig verschuldigde derdenprogrammatuur?	Voor de facturatie geldt de systematiek zoals tevens verduidelijkt in het antwoord op vraag 189. Van de eenmalige implementatievergoeding wordt 30% bij aanvang van de implementatie gefactureerd en de resterende 70% na integrale Acceptatie. De periodieke vergoeding voor de dienstverlening wordt vanaf de start van de operationele dienstverlening per kwartaal vooruit gefactureerd. Voor Derdenprogrammatuur geldt artikel 11 GIBIT 2025.

94	GIBIT 2025 art. 13.1 en 13.3 (pp.19–20); PvE A eisen 2.18 en 6.8–6.9 (pp.7,18–19)	Voor detectie en analyse kunnen statistische, geautomatiseerde of door derden geleverde AI/ML-modellen worden toegepast waarvan de interne werking niet volledig openbaar of technisch uitlegbaar is. Kan worden bevestigd dat de op grond van GIBIT artikel 13.3 gevraagde uitleg over individuele uitkomsten alleen verschuldigd is voor zover die met de feitelijk toegepaste technologie redelijkerwijs mogelijk is, zonder verstrekking van broncode, bedrijfsgeheimen of informatie waarop rechten van derden rusten?	Dit wordt ten dele bevestigd. Artikel 13.3 GIBIT 2025 blijft ongewijzigd van toepassing. De op grond van dit artikel te verstrekken uitleg dient de Aanbestedende dienst in staat te stellen individuele uitkomsten van een Algoritmische toepassing op een begrijpelijke wijze te kunnen duiden. Artikel 13.3 vereist niet zonder meer verstrekking van broncode, bedrijfsgeheimen of informatie waarop rechten van derden rusten. Dit laat onverlet dat Opdrachtnemer verantwoordelijk blijft voor het verstrekken van de informatie en uitleg die op grond van artikel 13 GIBIT 2025 is vereist. Het gebruik van technologie of modellen van derden beperkt deze verplichting niet. De GIBIT 2025 blijft op dit punt ongewijzigd van toepassing.
95	GIBIT 2025 art. 13.5 en 28 (pp.19,30); PvE A eisen 2.6 en 6.8 (pp.5,18)	Het controlerecht uit GIBIT artikel 13.5 strekt zich uit tot de correcte werking van algoritmen en de juistheid van de onderliggende gegevens. Kan worden bevestigd dat controles van door Microsoft of andere leveranciers beheerde, niet voor opdrachtnemer toegankelijke modellen worden beperkt tot redelijkerwijs beschikbare verificatiemiddelen, zonder onevenredige belasting of schending van intellectuele eigendomsrechten, bedrijfsgeheimen en contractuele verplichtingen aan derden?	Artikel 13.5 GIBIT 2025 blijft ongewijzigd van toepassing. Voor zover bij de uitvoering gebruik wordt gemaakt van door Microsoft of andere derden beheerde modellen waarop Opdrachtnemer geen rechtstreekse toegang heeft, vindt de controle plaats met gebruikmaking van de redelijkerwijs beschikbare verificatiemiddelen. Daarbij wordt rekening gehouden met gerechtvaardigde intellectuele eigendomsrechten en bedrijfsgeheimen van derden. Dit laat onverlet dat Opdrachtnemer verantwoordelijk blijft voor het voldoen aan de op hem rustende verplichtingen uit hoofde van artikel 13 GIBIT 2025 en voor het verlenen van de redelijkerwijs benodigde medewerking aan het controlerecht van de Aanbestedende dienst. De GIBIT 2025 blijft op dit punt ongewijzigd van toepassing.
96	GIBIT 2025 art. 14.1 (p.19); PvE A eisen 6.8–6.9 (pp.18–19)	Voor zover de aangeboden SOC-oplossing AI-functionaliteit bevat, welke objectieve criteria hanteert de gemeente om de door GIBIT artikel 14.1 verlangde nauwkeurigheid, robuustheid, cyberbeveiliging en mogelijkheden voor menselijk toezicht te beoordelen? Is de gemeente bereid te bevestigen dat opdrachtnemer aan deze bepaling voldoet door passende, aantoonbare en marktconforme beheersmaatregelen in te richten binnen zijn feitelijke invloedssfeer, in plaats van een onbegrensde resultaatgarantie?	De Aanbestedende dienst bevestigt dat artikel 14.1 GIBIT 2025 geen onbegrensde garantie op foutloze werking van AI-functionaliteit inhoudt. De beoordeling vindt plaats in relatie tot het Overeengekomen gebruik, de aard en het doel van de betreffende AI-functionaliteit, de daaraan verbonden risico's en de eisen uit de aanbestedingsstukken. Van Opdrachtnemer wordt verlangd dat passende en aantoonbare maatregelen zijn getroffen ten aanzien van nauwkeurigheid, robuustheid, cyberbeveiliging en menselijk toezicht, waarmee wordt voldaan aan artikel 14 GIBIT 2025 en de overige eisen uit de aanbestedingsstukken. Voor zover gebruik wordt gemaakt van AI-functionaliteit van derden, ontslaat dit Opdrachtnemer niet van de op hem rustende verplichtingen. De toepasselijke bepalingen inzake Derdenprogrammatuur blijven onverkort van toepassing. Artikel 14 GIBIT 2025 blijft ongewijzigd van toepassing.
97	GIBIT 2025 art. 14.3–14.4 (pp.19–20); PvE A eisen 6.8–6.9 (pp.18–19)	GIBIT artikel 14.3 legt de leverancier een zorgplicht op om te voorkomen dat opdrachtgever door eigen handelingen als AI-aanbieder kwalificeert. Kan worden bevestigd dat de verplichting van opdrachtnemer beperkt blijft tot tijdig informeren, passend instrueren en waarschuwen over risico’s die hij redelijkerwijs kan kennen en beïnvloeden, en dat wijzigingen of zelfstandig gebruik van AI-functionaliteit door de gemeente buiten die invloedssfeer niet voor rekening van opdrachtnemer komen? Welke partij bepaalt uiteindelijk de gebruiks- en risicoclassificatie?	Artikel 14.3 GIBIT 2025 blijft in de basis ongewijzigd van toepassing. Van Opdrachtnemer wordt verlangd dat hij de Aanbestedende dienst tijdig en adequaat informeert, instrueert en waarschuwt voor de voor hem redelijkerwijs kenbare risico's die verband houden met het beoogde gebruik van de betreffende AI-functionaliteit, en de maatregelen treft die op grond van artikel 14.3 van hem mogen worden verlangd. Voor zover de Aanbestedende dienst zelfstandig wijzigingen aanbrengt of de AI-functionaliteit aantoonbaar gebruikt buiten het Overeengekomen gebruik en zonder betrokkenheid van Opdrachtnemer, komen de gevolgen daarvan niet zonder meer voor rekening van Opdrachtnemer. De toepasselijke bepalingen van GIBIT 2025 blijven daarbij onverkort van toepassing. De juridische kwalificatie van het gebruik en de toepasselijke risicoclassificatie worden niet eenzijdig door één van Partijen bepaald, maar volgen uit de toepasselijke wet- en regelgeving en de feitelijke toepassing van het betreffende AI-systeem. Artikel 14 GIBIT 2025 blijft ongewijzigd van toepassing.

98	GIBIT 2025 art. 14.6–14.7 (p.20); PvE A eisen 2.10 en 6.8–6.9 (pp.6,18–19)	GIBIT artikelen 14.6 en 14.7 bevatten eisen aan gebeurtenislogging en traceerbaarheid van AI-systemen. Kan worden bevestigd dat deze plichten bij in de SIEM/SOC-dienst gebruikte standaard AI-functionaliteit van derden uitsluitend gelden voor zover de betreffende fabrikant die functionaliteit beschikbaar stelt en opdrachtnemer daarover feitelijke zeggenschap heeft? Welke meetbare mate van traceerbaarheid verlangt opdrachtgever naast de reguliere Sentinel- en SOC-auditlogging?	De artikelen 14.6 en 14.7 GIBIT 2025 blijven ongewijzigd van toepassing. Bij standaard AI-functionaliteit van derden wordt bij de invulling van de vereiste logging en traceerbaarheid rekening gehouden met de aard en de technische mogelijkheden van de betreffende functionaliteit. Het gebruik van Derdenprogrammatuur ontslaat Opdrachtnemer echter niet van de verplichtingen die op grond van de GIBIT 2025 en de aanbestedingsstukken op hem rusten. De Aanbestedende dienst stelt voor de in de SIEM/SOC-dienstverlening toegepaste AI-functionaliteit geen aanvullende afzonderlijke kwantitatieve eisen aan traceerbaarheid naast de eisen die reeds uit de GIBIT 2025 en de aanbestedingsstukken voortvloeien. De logging en beschikbare informatie moeten in ieder geval voldoende zijn om, binnen de kaders van artikel 14 GIBIT 2025, de relevante werking en uitkomsten van de toegepaste AI-functionaliteit te kunnen herleiden en controleren. De artikelen 14.6 en 14.7 GIBIT 2025 blijven ongewijzigd van toepassing.
99	GIBIT 2025 art. 14.9–14.10 (p.20); PvE A eis 6.8 (p.18)	GIBIT artikelen 14.9 en 14.10 verplichten tot ondersteuning en het beschikbaar stellen van informatie over AI-systemen. Kan worden bevestigd dat deze verplichtingen voor eventuele AI-componenten in de SIEM/SOC-dienst zien op technische uitleg en het aanleveren van bij opdrachtnemer beschikbare, redelijke productinformatie, en niet op het zelfstandig beoordelen van de juistheid van alle modeluitkomsten of het overnemen van de wettelijke transparantieverplichtingen van de gemeente?	Artikel 14.9 GIBIT 2025 ziet, voor zover van toepassing, op ondersteuning bij vragen over de werking en de technische interpretatie van de output van het AI-systeem. Artikel 14.10 GIBIT 2025 verplicht Opdrachtnemer de Aanbestedende dienst te voorzien van de informatie die noodzakelijk is om aan de op de Aanbestedende dienst rustende transparantieverplichtingen te kunnen voldoen. Deze bepalingen houden niet in dat Opdrachtnemer zelfstandig verantwoordelijk is voor de beoordeling van de juistheid van iedere individuele modeluitkomst of dat de op de Aanbestedende dienst rustende wettelijke transparantieverplichtingen als zodanig op Opdrachtnemer overgaan. De verplichtingen van Opdrachtnemer zijn echter niet beperkt tot uitsluitend reeds bij hem beschikbare productinformatie. Opdrachtnemer dient te voldoen aan hetgeen op grond van artikel 14.9 en 14.10 GIBIT 2025 van hem wordt verlangd. De GIBIT 2025 blijft op dit punt ongewijzigd van toepassing.
100	GIBIT 2025 art. 17.3 (p.21); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 17.3 maximeert aansprakelijkheid voor persoons- en zaakschade per gebeurtenis en per jaar, maar sluit gevolgschade en indirecte schade niet expliciet uit. Bent u bereid de aansprakelijkheid van partijen voor indirecte schade en gevolgschade, waaronder gederfde winst, gemiste besparingen, verminderde goodwill en bedrijfstagnatieschade, contractueel uit te sluiten voor zover wettelijk toegestaan?	Nee. De Aanbestedende dienst neemt de voorgestelde uitsluiting van indirecte schade en gevolgschade niet over. Artikel 17 GIBIT 2025 bevat reeds een regeling waarin de aansprakelijkheid voor persoons- en zaakschade en voor overige schade is begrensd. De Aanbestedende dienst ziet geen aanleiding om naast deze aansprakelijkheidsbeperkingen aanvullende schadecategorieën van vergoeding uit te sluiten. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
101	GIBIT 2025 art. 17.4 (p.21); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 17.4 maximeert aansprakelijkheid voor overige schade op tweemaal de jaarvergoeding per gebeurtenis en viermaal de jaarvergoeding per kalenderjaar. Gelet op de verhouding tot de contractwaarde en de aard van de managed-securitydienstverlening acht inschrijver dit risicoprofiel zwaar. Bent u bereid aansprakelijkheid voor overige directe schade te beperken tot maximaal eenmaal de jaarvergoeding per kalenderjaar, ongeacht het aantal gebeurtenissen, en indirecte schade uit te sluiten?	Nee. De Aanbestedende dienst neemt de voorgestelde beperking niet over. Artikel 17 GIBIT 2025 bevat reeds een regeling waarbij de aansprakelijkheid voor overige schade zowel per gebeurtenis als per kalenderjaar is gemaximeerd. De Aanbestedende dienst acht deze regeling passend bij de aard en risico's van de onderhavige dienstverlening en ziet geen aanleiding het aansprakelijkheidsmaximum verder te verlagen of aanvullende schadecategorieën van vergoeding uit te sluiten. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
102	GIBIT 2025 art. 17.5 (pp.21–22); PvE A eis 1.1 (p.3)	De aansprakelijkheidsbeperkingen uit GIBIT artikel 17.3 en 17.4 gelden op grond van artikel 17.5 niet voor onder meer aanspraken van derden wegens dood of letsel, intellectuele-eigendomsinbreuken en bepaalde toezichthoudersboetes. Bent u bereid deze uitzonderingen, voor zover juridisch toelaatbaar, eveneens onder evenredige en vooraf bepaalbare aansprakelijkheidslimieten te brengen, met behoud van een passende uitzondering voor opzet en grove schuld?	Nee. De Aanbestedende dienst neemt de voorgestelde wijziging niet over. Artikel 17 GIBIT 2025 bevat een samenhangende regeling waarin de aansprakelijkheid in beginsel is gemaximeerd en waarin voor specifieke omstandigheden is bepaald dat deze beperkingen niet van toepassing zijn. De Aanbestedende dienst ziet geen aanleiding om de in artikel 17.5 GIBIT 2025 opgenomen uitzonderingen alsnog aan aanvullende aansprakelijkheidslimieten te onderwerpen. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.

103	GIBIT 2025 art. 17.6 (p.22); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 17.6 sluit aansprakelijkheidsbegrenzing expliciet uit voor de vrijwaring inzake belasting-, zorgverzekerings- en sociale verzekeringsverplichtingen voor personeel. Bent u bereid deze vrijwaring te laten vallen onder de maxima van artikel 17.3 en 17.4, nu een onbeperkte vrijwaring niet in verhouding staat tot de overeengekomen dienstverlening?	Nee. De Aanbestedende dienst neemt de voorgestelde wijziging niet over. Artikel 17.6 GIBIT 2025 bepaalt expliciet dat de verplichtingen met betrekking tot het personeel van Opdrachtnemer uit hoofde van de belasting-, zorgverzekerings- en socialeverzekeringswetgeving voor rekening van Opdrachtnemer komen en dat de aansprakelijkheidsbeperkingen van artikel 17 daarop niet van toepassing zijn. De Aanbestedende dienst ziet geen aanleiding van deze in de GIBIT 2025 opgenomen risicoverdeling af te wijken. Artikel 17.6 GIBIT 2025 blijft ongewijzigd van toepassing.
104	GIBIT 2025 art. 18.1–18.2 (p.22); GIBIT art. 17.3–17.5 (pp.21–22)	GIBIT artikelen 18.1 en 18.2 verlangen passende beroeps- en bedrijfsaansprakelijkheidsverzekeringen met dekking voor de in artikel 17 genoemde risico's. Kan de gemeente bevestigen dat de polisvoorwaarden van gebruikelijke, aantoonbaar passende bedrijfs- en beroepsaansprakelijkheidsverzekeringen worden geaccepteerd en dat een verzekeringscertificaat van de verzekeringsmakelaar volstaat als bewijs, mede in samenhang met eventuele naar aanleiding van de Nota van Inlichtingen aangepaste aansprakelijkheidslimieten?	De artikelen 18.1 en 18.2 GIBIT 2025 blijven ongewijzigd van toepassing. De door Opdrachtnemer aangehouden bedrijfs- en beroepsaansprakelijkheidsverzekeringen dienen naar aard en omvang passend te zijn voor de op grond van de Overeenkomst en artikel 17 GIBIT 2025 bestaande aansprakelijkheidsrisico's. Een verzekeringscertificaat of verzekeringsverklaring van de verzekeraar of verzekeringsmakelaar kan als bewijs volstaan, mits daaruit genoegzaam blijkt dat wordt voldaan aan de eisen van artikel 18 GIBIT 2025. De Aanbestedende dienst behoudt zich het recht voor om, indien daartoe aanleiding bestaat, nadere bewijsstukken te verlangen. De artikelen 17 en 18 GIBIT 2025 blijven ongewijzigd van toepassing.
105	GIBIT 2025 art. 19.4 (p.22); Leidraad §6.5 (p.27)	Artikel 19.4 GIBIT staat toe de inhoud van de overeenkomst met andere gemeenten en samenwerkingsverbanden te delen. De inschrijving en de uitwerking van de SOC-dienst kunnen vertrouwelijke prijs-, security- en bedrijfsinformatie bevatten. Bent u bereid deze bepaling te beperken tot gegevens die noodzakelijk zijn voor de publieke taak, onder uitsluiting van bedrijfsgeheimen en vertrouwelijke, inschrijverspecifieke beveiligingsinformatie zonder voorafgaande toestemming van opdrachtnemer?	Nee. De Aanbestedende dienst neemt de voorgestelde beperking niet over. Artikel 19.4 GIBIT 2025 blijft ongewijzigd van toepassing. De Aanbestedende dienst zal bij toepassing van artikel 19.4 zorgvuldig omgaan met als vertrouwelijk aangemerkte bedrijfs-, prijs- en beveiligingsinformatie en deze niet verder delen dan in het kader van de in artikel 19.4 bedoelde informatie-uitwisseling noodzakelijk en gerechtvaardigd is. Een voorafgaande toestemming van Opdrachtnemer wordt daarbij niet als aanvullende voorwaarde gesteld. De overige toepasselijke geheimhoudingsverplichtingen en wettelijke verplichtingen ten aanzien van vertrouwelijke informatie blijven onverkort van toepassing.
106	GIBIT 2025 art. 19.6 (pp.22–23); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 19.6 verbindt aan schending van geheimhouding een direct opeisbare boete van € 10.000 per overtreding naast het recht op schadevergoeding. Bent u bereid deze boete als gefixeerde schadevergoeding aan te merken voor dezelfde overtreding, zodat samenloop en dubbele financiële sanctionering worden voorkomen?	Nee. De Aanbestedende dienst neemt de voorgestelde wijziging niet over. Artikel 19.6 GIBIT 2025 voorziet uitdrukkelijk in een direct opeisbare boete van € 10.000 per overtreding, naast het recht op vergoeding van de daadwerkelijk geleden schade. De Aanbestedende dienst ziet geen aanleiding om deze boete aan te merken als gefixeerde schadevergoeding of het recht op aanvullende schadevergoeding te beperken. Artikel 19.6 GIBIT 2025 blijft ongewijzigd van toepassing.
107	GIBIT 2025 art. 20.2 (p.23); PvE A eis 8.6 (p.21)	GIBIT artikel 20.2 kent een beperkte omschrijving van overmacht. Kan de gemeente bevestigen dat niet-toerekenbare uitval van algemene nuts- of telecomvoorzieningen, grootschalige incidenten bij Microsoft of andere platformleveranciers en andere aantoonbaar buiten de redelijke invloedssfeer van opdrachtnemer gelegen verstoringen als overmacht dan wel als uitgesloten oorzaak voor SLA-toerekening worden behandeld, mits opdrachtnemer passende continuïteitsmaatregelen heeft getroffen?	Artikel 20 GIBIT 2025 blijft ongewijzigd van toepassing. Of in een concreet geval sprake is van overmacht wordt beoordeeld aan de hand van artikel 20 GIBIT 2025 en de omstandigheden van het betreffende geval. Voor de toerekening onder de SLA geldt het bepaalde in het Programma van Eisen. Uitval van gemeentelijke systemen, logbronnen of onderliggende Microsoft-clouddiensten wordt niet aan Opdrachtnemer toegerekend, tenzij Opdrachtnemer de uitval heeft veroorzaakt of onvoldoende passende maatregelen heeft getroffen. Voor overige verstoringen wordt overeenkomstig de GIBIT 2025, het Programma van Eisen en de nader vast te stellen SLA beoordeeld in hoeverre deze aan Opdrachtnemer kunnen worden toegerekend. Artikel 20 GIBIT 2025 en de betreffende bepalingen uit het Programma van Eisen blijven ongewijzigd van toepassing.

108	GIBIT 2025 art. 21.7 (pp.23–24); PvE A eisen 2.23 en 6.3 (pp.8,18)	GIBIT artikel 21.7 verplicht opdrachtnemer tot vrijwaring wegens inbreuk op intellectuele-eigendomsrechten van derden. Voor standaardprogrammatuur zoals Microsoft Sentinel en eventuele softwarecomponenten van andere fabrikanten kan opdrachtnemer de rechten en vrijwaringsvoorwaarden van die rechthebbenden niet zelfstandig wijzigen. Bent u bereid deze vrijwaring te beperken tot voor zover de inbreuk is veroorzaakt door door opdrachtnemer zelf ontwikkelde of gewijzigde onderdelen, dan wel de aansprakelijkheidsmaxima van GIBIT artikel 17 van toepassing te verklaren?	Nee. De Aanbestedende dienst neemt de voorgestelde beperking niet over. Artikel 21 GIBIT 2025 bevat een specifieke regeling inzake intellectuele-eigendomsrechten en aanspraken van derden. Het gebruik van Derdenprogrammatuur doet als zodanig geen afbreuk aan de verplichtingen van Opdrachtnemer uit hoofde van artikel 21.7 GIBIT 2025. De GIBIT 2025 voorziet reeds in specifieke bepalingen voor Derdenprogrammatuur en in uitzonderingen op de vrijwaring, onder meer indien de gestelde inbreuk verband houdt met door de Aanbestedende dienst ter beschikking gestelde programmatuur of materialen, dan wel met door de Aanbestedende dienst zonder schriftelijke toestemming van Opdrachtnemer aangebrachte wijzigingen. De Aanbestedende dienst ziet geen aanleiding de vrijwaring te beperken tot door Opdrachtnemer zelf ontwikkelde of gewijzigde onderdelen of daarop de aansprakelijkheidsmaxima van artikel 17.3 en 17.4 GIBIT 2025 van toepassing te verklaren. De artikelen 17, 21 en 23 GIBIT 2025 blijven ongewijzigd van toepassing.
109	GIBIT 2025 art. 21.8 en 21.10 (p.24); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 21.8 verplicht reeds bij een dreigende IE-aanspraak tot maatregelen en artikel 21.10 biedt bij een enkele aanspraak van een derde ruimte voor ontbinding. Kan de gemeente bevestigen dat ingrijpende herstel- en ontbindingsrechten pas worden ingeroepen wanneer een daadwerkelijke, objectief onderbouwde IE-inbreuk is vastgesteld die opdrachtnemer niet binnen een redelijke termijn kan wegnemen, en dat een onbewezen claim of enkel risico daartoe niet volstaat?	Nee. De Aanbestedende dienst neemt de voorgestelde beperking niet over. De artikelen 21.8 en 21.10 GIBIT 2025 regelen de rechten en verplichtingen van Partijen indien sprake is van een (dreigende) inbreuk op intellectuele-eigendomsrechten respectievelijk een aanspraak van een derde. De Aanbestedende dienst ziet geen aanleiding deze rechten afhankelijk te stellen van de voorwaarde dat een daadwerkelijke IE-inbreuk reeds definitief is vastgesteld of dat Opdrachtnemer eerst in alle gevallen een aanvullende hersteltermijn wordt geboden. De in artikel 21 GIBIT 2025 opgenomen voorwaarden en mogelijkheden tot het treffen van maatregelen blijven ongewijzigd van toepassing. Artikel 21 GIBIT 2025 blijft ongewijzigd van toepassing.
110	GIBIT 2025 art. 25.1–25.2 (pp.27–28); PvE A eisen 2.16 en 2.23 (pp.7–8)	GIBIT artikel 25.1 verlangt een volledige Software Bill of Materials voor de gehele ICT-prestatie, terwijl de oplossing gebruikmaakt van Microsoft Sentinel en eventueel andere niet door opdrachtnemer ontwikkelde platforms. Kan worden bevestigd dat opdrachtnemer uitsluitend gehouden is de redelijkerwijs beschikbare SBOM- en keteninformatie van eigen onderdelen en van door derden beschikbaar gestelde componenten te leveren? Welke concrete informatie verlangt de gemeente onder "privacy- en beveiligingsrisico's" in dit overzicht?	De SBOM ziet op de wezenlijke softwarecomponenten die onderdeel uitmaken van de geleverde ICT Prestatie. Dit omvat zowel eigen softwarecomponenten als relevante Derdenprogrammatuur. Voor Derdenprogrammatuur en andere door derden beheerde componenten verstrekt Opdrachtnemer de beschikbare SBOM- en keteninformatie en maakt hij eventuele beperkingen in de beschikbaarheid daarvan inzichtelijk.
111	GIBIT 2025 art. 27.10 (pp.28–29); Bijlage G art. 3 (p.37)	Artikel 27.10 GIBIT biedt ontbindingsmogelijkheden maar bepaalt niet expliciet dat reeds geleverde, niet ongedaan te maken SOC-diensten naar de stand van uitvoering worden afgerekend. Bent u bereid vast te leggen dat bij (gedeeltelijke) ontbinding de tot dat moment daadwerkelijk verrichte en aanvaarde werkzaamheden en verstrekte gebruiksrechten overeenkomstig de overeengekomen tarieven worden vergoed, voor zover wettelijk en contractueel passend?	Artikel 27 GIBIT 2025 blijft ongewijzigd van toepassing. Bij een gehele of gedeeltelijke ontbinding vindt de financiële afwikkeling plaats overeenkomstig de GIBIT 2025 en het toepasselijke recht. Voor zover prestaties naar hun aard niet ongedaan kunnen worden gemaakt, worden de gevolgen daarvan overeenkomstig de toepasselijke contractuele en wettelijke bepalingen afgewikkeld. Dit betekent niet dat Opdrachtnemer zonder meer aanspraak heeft op volledige vergoeding tegen de overeengekomen tarieven, indien de betreffende prestaties niet of niet behoorlijk aan de Overeenkomst beantwoorden. De Aanbestedende dienst ziet geen aanleiding artikel 27 GIBIT 2025 op dit punt aan te passen.
112	GIBIT 2025 art. 27.11 (p.29); Bijlage G art. 1.3 (pp.36–37)	GIBIT artikel 27.11 verleent opdrachtgever gedurende twaalf maanden na constatering van bepaalde omstandigheden een bijzonder ontbindingsrecht. Bent u bereid deze periode terug te brengen tot drie maanden na schriftelijke kennisneming van de betreffende omstandigheid, zodat over de voortzetting van de langdurige SIEM/SOC-overeenkomst niet onnodig lang onzekerheid bestaat?	Nee. De Aanbestedende dienst neemt de voorgestelde verkorting van de termijn niet over. Artikel 27.11 GIBIT 2025 voorziet in een bijzonder ontbindingsrecht dat gedurende de daarin opgenomen termijn kan worden uitgeoefend indien zich één van de in dat artikel genoemde omstandigheden voordoet. De Aanbestedende dienst ziet geen aanleiding deze termijn te verkorten. Artikel 27.11 GIBIT 2025 blijft ongewijzigd van toepassing.

113	GIBIT 2025 art. 27.11 onder v, vi en xi (pp.29–30); Bijlage G art. 4 (p.37)	Kunt u voor de bijzondere ontbindingsgronden van GIBIT artikel 27.11 nader afbakenen dat gewone concernreorganisaties of wijzigingen in zeggenschap zonder nadelige gevolgen voor de uitvoering, beslagen die de continuïteit niet raken en de algemeen geformuleerde grond inzake de publieke positie van opdrachtgever uitsluitend tot ontbinding kunnen leiden wanneer objectief aantoonbare, zwaarwegende omstandigheden bestaan die voortzetting van de overeenkomst daadwerkelijk onaanvaardbaar maken?	Nee. De Aanbestedende dienst neemt de voorgestelde nadere beperking niet over. Artikel 27.11 GIBIT 2025 bevat specifieke omstandigheden waaronder de Aanbestedende dienst bevoegd is de Overeenkomst te ontbinden en blijft ongewijzigd van toepassing. Of zich een in artikel 27.11 bedoelde omstandigheid voordoet, wordt beoordeeld aan de hand van de concrete feiten en omstandigheden van het betreffende geval. De Aanbestedende dienst ziet geen aanleiding om aan de toepassing van artikel 27.11 aanvullende voorwaarden of drempels te verbinden die niet reeds uit de GIBIT 2025 voortvloeien.
114	GIBIT 2025 art. 27.12 (p.30); Bijlage G art. 1.3 (pp.36–37)	Artikel 27.12 GIBIT maakt bij een wegens aanbestedingsrechtelijke onrechtmatigheid noodzakelijke ontbinding een uitzondering op de financiële gevolgen indien de oorzaak mede aan opdrachtnemer toerekenbaar is. Kan de gemeente bevestigen dat in gevallen van medeverantwoordelijkheid de financiële afrekening en eventuele schadeverdeling naar rato van de daadwerkelijk aan ieder der partijen toe te rekenen oorzaak plaatsvinden, in plaats van dat iedere beperkte medeschuld automatisch tot volledige uitsluiting van vergoeding leidt?	Nee. De Aanbestedende dienst neemt de voorgestelde wijziging niet over. Artikel 27.12 GIBIT 2025 bevat een specifieke regeling voor de financiële gevolgen van een ontbinding die noodzakelijk is wegens aanbestedingsrechtelijke onrechtmatigheid, waarbij tevens rekening is gehouden met de situatie waarin de oorzaak daarvan mede aan Opdrachtnemer kan worden toegerekend. De Aanbestedende dienst ziet geen aanleiding om hieraan een aanvullende pro-rataregeling of causaliteitsverdeling toe te voegen. Artikel 27.12 GIBIT 2025 blijft ongewijzigd van toepassing.
115	GIBIT 2025 art. 28.1–28.6 (pp.30–31); PvE A eis 3.4 (p.10); Verwerkersovereenkomst art. 4.2 (p.2)	De aanbestedingsstukken voorzien in reguliere audits, terwijl GIBIT artikel 28.1 een aanvullend controlemechanisme biedt. Bent u bereid het aantal reguliere fysieke audits in beginsel tot één per contractjaar te beperken, actuele ISO 27001-/ISAE-/SOC-assurancerapportages als gebruikelijk alternatief te aanvaarden wanneer die voldoende zekerheid bieden, en de onafhankelijke auditor vooraf in onderling overleg te laten aanwijzen, behoudens wettelijke of incidentgerelateerde auditrechten?	De Aanbestedende dienst ziet geen aanleiding het in het Programma van Eisen opgenomen maximum van twee reguliere audits per contractjaar te wijzigen. Wettelijke auditrechten en incidentele controles naar aanleiding van onder meer calamiteiten, beveiligingsincidenten, substantiële wijzigingen of compliance-vraagstukken blijven hiervan uitgezonderd. Actuele en relevante certificeringen en onafhankelijke assurance-rapportages, waaronder ISO 27001-, ISAE- of SOC-rapportages, kunnen bij de invulling van het controlerecht worden betrokken en kunnen, voor zover deze naar het oordeel van de Aanbestedende dienst voldoende zekerheid bieden over het betreffende onderwerp, aanleiding zijn de omvang van een aanvullende audit te beperken. De Aanbestedende dienst stemt niet in met de voorwaarde dat een onafhankelijke auditor uitsluitend in onderling overleg kan worden aangewezen. Bij de uitvoering van controles wordt overeenkomstig artikel 28 GIBIT 2025 zorgvuldig rekening gehouden met de gerechtvaardigde belangen van Opdrachtnemer. Het Programma van Eisen en artikel 28 GIBIT 2025 blijven op dit punt ongewijzigd van toepassing.
116	GIBIT 2025 art. 28.7 (p.31); PvE A eis 3.4 (p.10)	GIBIT artikel 28.7 biedt opdrachtgever aanvullende mogelijkheden tot beveiligingscontrole door het CSIRT. Kan worden bevestigd dat, wanneer opdrachtnemer onder relevant wettelijk toezicht staat en reeds periodieke onafhankelijke securitycertificeringen en auditrapportages verstrekt, deze informatie vooraf bij de proportionaliteitsbeoordeling van een aanvullende CSIRT-controle wordt betrokken, behoudens wettelijke verplichtingen of een concreet veiligheidsincident?	Bij de beoordeling of en in welke omvang een aanvullende controle op grond van artikel 28.7 GIBIT 2025 noodzakelijk is, kan de Aanbestedende dienst rekening houden met relevant wettelijk toezicht en actuele, onafhankelijke certificeringen en audit- of assurancerapportages van Opdrachtnemer, voor zover deze voldoende zekerheid bieden over het onderwerp en de reikwijdte van de voorgenomen controle. Dit beperkt het controlerecht van de Aanbestedende dienst en het CSIRT op grond van artikel 28.7 GIBIT 2025 niet, waaronder in geval van een wettelijke verplichting, een beveiligingsincident of wanneer de beschikbare informatie onvoldoende zekerheid biedt. Artikel 28 GIBIT 2025 blijft ongewijzigd van toepassing.
117	Aanbestedingsdocument §3.2.1 (p. 15); Bijlage E	In paragraaf 3.2.1 staat vermeld dat de twee kerncompetenties met aparte referentieopdrachten moeten worden aangetoond. Betekent dit dat een enkele, geïntegreerde referentieopdracht bij een Nederlandse (semi)publieke organisatie, waarin zowel de implementatie en het beheer van Microsoft Sentinel als de 24/7 SOC-dienstverlening volledig en succesvol zijn uitgevoerd, niet mag worden ingezet om beide kerncompetenties gelijktijdig aan te tonen? Zo ja, wat is de inhoudelijke noodzaak van het aanleveren van twee afzonderlijke contracten?	De aanbestedende dienst verduidelijkt dat één referentieopdracht voor beide kerncompetenties mag worden gebruikt, mits uit die referentie afzonderlijk en aantoonbaar blijkt dat aan alle eisen van zowel kerncompetentie 1 als kerncompetentie 2 wordt voldaan. De opdrachtgever verlangt dus ervaring met zowel de implementatie en het beheer van Microsoft Sentinel als de 24/7 SOC-dienstverlening, maar eist niet dat deze ervaring uit twee verschillende contracten afkomstig is. De inschrijver moet per kerncompetentie duidelijk maken welk onderdeel van de referentie de betreffende ervaring aantoont. Dit voorkomt dat een passende, geïntegreerde opdracht alleen vanwege de contractvorm buiten beschouwing blijft. De mogelijkheid om één referentie voor meerdere kerncompetenties te gebruiken sluit aan bij het aanbestedingsrechtelijk uitgangspunt dat een referentie meerdere kerncompetenties kan aantonen.

118	Bijlage A, eisen 2.2 en 2.13 (pp. 4, 6)	In eis 2.2 worden passende aanvullende use-cases "out of the box" verlangd. Kan worden bevestigd dat onder deze "out-of-the-box"-functionaliteit tevens de reeds bestaande detectiecontent van Opdrachtnemer wordt verstaan die binnen Microsoft Sentinel moet worden geconfigureerd of getuned? Kan de gemeente daarnaast bevestigen dat het eventueel noodzakelijk ontwikkelen van nieuwe, klantspecifieke connectoren, geavanceerde parsers of klantspecifieke detectielogica die buiten de veertien initiële logbronnen vallen, uitsluitend na afzonderlijke schriftelijke opdracht en prijsafspraak plaatsvindt?	Eis 2.2 verlangt dat de oplossing voor elk van de veertien genoemde logbronnen passende aanvullende use-case-dekking out of the box ondersteunt. Dit omvat ook reeds bestaande generieke detectiecontent van de opdrachtnemer, voor zover die geschikt is voor de betreffende bronnen en als onderdeel van de aangeboden standaarddienstverlening in Microsoft Sentinel wordt geconfigureerd of getuned. De noodzakelijke configuratie en tuning voor de overeengekomen logbronnen vallen binnen de aangeboden dienstverlening.
119	Aanbestedingsdocument §1.1.2; Bijlage A, eisen 2.20, 8.14 en 8.22 (pp. 4, 7, 22)	In paragraaf 1.1.2 staat dat responsacties zonder vooraf vastgelegde bevoegdheden en mandaten zijn uitgesloten. Kan de gemeente bevestigen dat ingrijpende containment- en herstelacties door het SOC (zoals het isoleren van hosts, het blokkeren van netwerkverkeer of het intrekken van accounts) uitsluitend plaatsvinden op basis van vooraf tijdens de implementatiefase expliciet schriftelijk overeengekomen mandaten en playbooks, en dat de uiteindelijke bestuurlijke en operationele regie bij niet-gemandateerde scenario's te allen tijde bij de gemeente berust?	Ja. De opdrachtgever bevestigt dat ingrijpende responsacties in de gemeentelijke omgeving, zoals het isoleren van hosts, het blokkeren van netwerkverkeer of het intrekken van accounts, uitsluitend mogen worden uitgevoerd op basis van vooraf schriftelijk vastgelegde bevoegdheden en mandaten. Deze kunnen tijdens de implementatie per use-case of responsactie worden vastgelegd, bijvoorbeeld in het DAP en de bijbehorende playbooks.
120	PvE A, eisen 2.2, 2.13 en 5.5; Bijlage F1, regels 14–27	Kunt u voor alle in eis 2.2 genoemde logbronnen per bron het actuele product, de leverancier, editie of licentieniveau, versie, deploymentvorm en de relevante aantallen tenants, omgevingen, gebruikers, assets of apparaten verstrekken?	Het betreft een tenant, de aantallen gebruikers, werkplekken, servers worden in het prijsblad opgenomen. Versienummers en dergelijke zijn momenteel niet voor handen.
121	PvE A, eisen 2.2 en 5.5; Bijlage F1, regels 14–27	Kunt u per logbron het gemeten gemiddelde en pieklogvolume verstrekken?	Hier is binnen de gemeente nu geen voorziening voor. Gemeente laat zich gaarne adviseren welke log-settings een doeltreffend balans tussen inzicht en volume treffen. Aantallen firewalls en andere security appliances zullen benoemd worden in het gewijzigde prijzenblad dat als bijlage 1 bij deze Nota van Inlichtingen is toegevoegd.
122	PvE A, eisen 2.2 en 5.5; Bijlage F1, regels 14–27	Welke bewaartermijn moet per logbron voor calculatie en inrichting worden aangehouden?	Zie vraag en antwoord 34
123	PvE A, eisen 2.13 en 5.5; Bijlage F1, regels 14–27	Kunt u per logbron aangeven of een ondersteunde standaardconnector of API beschikbaar is, welke toegangsrechten nodig zijn en of de bron technisch en contractueel aansluitgereed is?	De logbronnen betreffen voornamelijk generieke inzet van de genoemde technische oplossingen. De relevante logbronnen kennen standaard connectoren in Sentinel. Waar dit niet het geval is is de API beschikbaar.
124	PvE A, eisen 2.2, 2.16 en 5.5	Kunt u de actuele aantallen per Microsoft 365-licentieniveau, waaronder E3 en E5, en per aanvullende Defender- of securitylicentie voor gebruikers, endpoints en servers verstrekken?	Dit wordt als aantallen in het prijsblad gekwantificeerd.
125	PvE A, eisen 2.16 en 5.5	Kunt u de aanwezige Azure-subscriptions en Log Analytics-workspaces en de huidige Microsoft Sentinel-configuratie, dataretentie en commitment tier verstrekken?	nee, er zijn geen bestaande sentinel/log analytics workspaces in place. Deze configuratie wordt verwacht van de dienstverlener. Kosten hiervan worden door de gemeente rechtstreeks gedragen.
126	GIBIT 2025 - Artikel 3 lid 2 i)	Onder (i) In plaats van "Doelstellingen" beter om te spreken over bijvoorbeeld "Het door Opdrachtgever beoogde gebruik van de Prestatie, zoals dat door de Opdrachtgever kenbaar is gemaakt." Doelstellingen kunnen tegenstrijdig zijn. Hier ligt een taak voor de Opdrachtgever om de leverancier daarover te informeren. Kunt u hiermee instemmen?	Nee, niet akkoord.

127	GIBIT 2025 - Artikel 3 lid 3	Graag de volgende woorden toevoegen aan artikel 3 lid 3: "en Opdrachtgever zal ook (proactief) de Leverancier tijdig van adequate informatie voorzien." Goede informatieverschaffing door Opdrachtgever is essentieel voor goede overeenstemming tussen partijen over de ICT- Prestatie. Kunt u hiermee instemmen?	De opdrachtgever stemt niet in met de voorgestelde aanvulling.
128	GIBIT 2025 - Artikel 17	In zijn geheel vervangen door: 17.1Partijen aanvaarden over en weer slechts wettelijke verplichtingen tot schadevergoeding voor zover dat uit dit artikel en de navolgende artikelen blijkt. 17.2Partijen zijn aansprakelijk voor de door de andere partij geleden directe schade indien de aanspraken zijn ontstaan: •ten gevolge van een toerekenbaar tekortschieten in de nakoming van een of meerdere verplichtingen in haar verplichtingen jegens de andere partij; •ten gevolge van een buitencontractueel toerekenbaar handelen of nalaten bij de werkzaamheden die de andere partij haar medewerkers en/of haar onderaannemers verricht ter uitvoering van deze Overeenkomst. 17.3Aansprakelijkheid van Partijen voor indirecte schade, daaronder begrepen gevolgschade, gederfde winst, gemiste besparingen, verlies van gegevens, gegevensbestanden en schade door bedrijfsstagnatie, is nadrukkelijk uitgesloten. 17.4Dit artikel is van overeenkomstige toepassing op vrijwaring. 17.5De Partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen is tegenover de andere Partij uitsluitend aansprakelijk voor de door de andere Partij geleden of te lijden directe schade. 17.6De hierboven bedoelde aansprakelijkheid voor directe schade is, per gebeurtenis, beperkt tot een bedrag van € 1.000.000,- per gebeurtenis, waarbij een reeks van samenhangende gebeurtenissen aangemerkt zal worden als één gebeurtenis, zulks met een maximum van € 2.000.000,- per kalenderjaar. Onder directe schade wordt uitsluitend verstaan: - schade aan producten en functies, waaronder in elk geval verstaan	Nee. De Aanbestedende dienst stemt niet in met de voorgestelde vervanging van artikel 17 GIBIT 2025. Artikel 17 GIBIT 2025 bevat reeds een samenhangende en wederkerige regeling voor de aansprakelijkheid van Partijen, met afzonderlijke aansprakelijkheidsmaxima voor persoons- en zaakschade en overige schade en met specifiek benoemde uitzonderingen op deze beperkingen. De Aanbestedende dienst acht deze regeling, mede gelet op de aard en risico's van de onderhavige SIEM/SOC-dienstverlening, passend en ziet geen aanleiding deze te vervangen door de voorgestelde regeling, de aansprakelijkheid te beperken tot uitsluitend directe schade of de in GIBIT 2025 opgenomen uitzonderingen op de aansprakelijkheidsbegrenzing te beperken. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
129	GIBIT 2025 - Artikel 25 lid 1	Kan Opdrachtgever bevestigen dat de verplichting tot het verstrekken van een Software Bill of Materials uitsluitend ziet op door Leverancier zelf ontwikkelde softwarecomponenten en niet op onderliggende netwerk-, infrastructuur of platformcomponenten?	De SBOM ziet op de wezenlijke softwarecomponenten die onderdeel uitmaken van de geleverde ICT Prestatie. Dit omvat zowel eigen softwarecomponenten als relevante Derdenprogrammatuur. Voor Derdenprogrammatuur en andere door derden beheerde componenten verstrekt Opdrachtnemer de beschikbare SBOM- en keteninformatie en maakt hij eventuele beperkingen in de beschikbaarheid daarvan inzichtelijk.
130	GIBIT 2025 - Artikel 25 lid 1	Toevoegen aan artikel: “De SBOM wordt uitsluitend op hoofdlijnen verstrekt en omvat geen gedetailleerde broncode-, configuratie- of architectuurinformatie” Kunt u hiermee instemmen?	"De SBOM ziet op de wezenlijke softwarecomponenten die onderdeel uitmaken van de geleverde ICT Prestatie. Dit omvat zowel eigen softwarecomponenten als relevante Derdenprogrammatuur. Voor Derdenprogrammatuur en andere door derden beheerde componenten verstrekt Opdrachtnemer de beschikbare SBOM- en keteninformatie en maakt hij eventuele beperkingen in de beschikbaarheid daarvan inzichtelijk. De Aanbestedende dienst kan instemmen met deze uitleg, maar acht een tekstuele aanvulling niet noodzakelijk. Artikel 25 GIBIT 2025 verplicht niet tot het verstrekken van broncode, configuratie- of gedetailleerde architectuurinformatie. De SBOM wordt op hoofdlijnen en proportioneel verstrekt overeenkomstig artikel 25 GIBIT 2025. Artikel 25 GIBIT 2025 blijft ongewijzigd van toepassing."

131	GIBIT 2025 - Artikel 25	Toevoegen aan artikel: “De SBOM wordt uitsluitend gebruikt voor interne risicobeoordeling en mag niet met derden worden gedeeld, behoudens het genoemde in artikel 25.5” Kunt u hiermee instemmen?	De Aanbestedende dienst acht de voorgestelde toevoeging niet noodzakelijk. Artikel 25 GIBIT 2025 voorziet reeds in de vertrouwelijke behandeling van de SBOM en bevat bepalingen ten aanzien van het delen daarvan. De Aanbestedende dienst ziet geen aanleiding hier aanvullende beperkingen aan toe te voegen. Artikel 25 GIBIT 2025 blijft ongewijzigd van toepassing.
132	Uitvoeringsprotocol Social Return	Het Uitvoeringsprotocol bepaalt dat voor de verantwoording van een stage een door de school erkende en ondertekende stageovereenkomst moet worden overgelegd waarin het opleidingsniveau is opgenomen. Inschrijver werkt met stageovereenkomsten tussen inschrijver en stagiair, waarbij het opleidingsniveau niet in de overeenkomst wordt vermeld. Kan opdrachtgever bevestigen dat ook alternatieve bewijsstukken, naast de stageovereenkomst, worden geaccepteerd om de stage en het betreffende opleidingsniveau aantoonbaar te maken?	Nee, dit kan vooraf niet worden bevestigd. De praktische invulling en verantwoording van de Social Return-verplichting wordt na gunning door Opdrachtnemer afgestemd met het Adviespunt Social Return. Daarbij kan tevens worden besproken welke bewijsstukken voor de betreffende invulling benodigd zijn. Het Uitvoeringsprotocol Social Return blijft ongewijzigd van toepassing.
133	Uitvoeringsprotocol Social Return	Kan opdrachtgever toelichten of een geldige PSO-certificering van de opdrachtnemer zelf kan worden gewaardeerd binnen de Social Return-verplichting, bijvoorbeeld door een gehele of gedeeltelijke vermindering van het te realiseren Social Return-bedrag?	Nee, dit kan vooraf niet worden bevestigd. Een PSO-certificering van Opdrachtnemer leidt niet automatisch tot een gehele of gedeeltelijke vermindering van de Social Return-verplichting. De praktische invulling van de Social Return-verplichting wordt na gunning door Opdrachtnemer afgestemd met het Adviespunt Social Return. In dat kader kan tevens worden besproken in hoeverre relevante Social Return-activiteiten van Opdrachtnemer binnen de kaders van het Uitvoeringsprotocol kunnen worden gewaardeerd. Het Uitvoeringsprotocol Social Return blijft ongewijzigd van toepassing.
134	Uitvoeringsprotocol Social Return	Inschrijver begrijpt dat de Gemeente Vijfherenlanden werkt met het systeem InterPactum ter controle van afspraken over Social Return. Inschrijver is van mening dat zij in strijd met de AVG handelt als zij gegevens van medewerkers op persoonsniveau aanlevert aan de Gemeente (al dan niet via InterPactum) omdat de Social Return afspraken ook op een andere manier kunnen worden gecontroleerd, zonder (bijzondere) persoonsgegevens te delen. Het is m.a.w. niet noodzakelijk om (gezondheids)gegevens op persoonsniveau te delen via InterPactum ter controle van Social Return afspraken en als Inschrijver dit wel zou doen handelt zij in strijd met de AVG. Staat de Gemeente open voor alternatieve oplossingen waarbij de Social Return afspraken gecontroleerd worden, zoals bijvoorbeeld het aanleveren van een verklaring van een onafhankelijke auditor, steekproeven, inzage op verzoek, waarna goedkeuring alsnnog verloopt via het systeem InterPactum ? Verwijzen naar een privacy-protocol is daarbij voor ons geen passend, inhoudelijk antwoord, omdat we mogelijk anders aankijken tegen de wijze waarop wij gegevens van onze medewerkers (niet) kunnen delen en wij daarom willen kijken met elkaar naar een andere werkwijze waarbij dit niet nodig is.	"De Aanbestedende dienst onderschrijft dat bij de verantwoording van Social Return zorgvuldig en overeenkomstig de toepasselijke privacywetgeving met persoonsgegevens moet worden omgegaan. De Aanbestedende dienst bevestigt niet dat de in het Uitvoeringsprotocol voorziene wijze van verantwoording in strijd is met de AVG. De exacte praktische invulling en verantwoording van de Social Return-verplichting wordt na gunning tussen Opdrachtnemer en het Adviespunt Social Return afgestemd. Daarbij kan tevens worden bezien op welke wijze de benodigde controle en verantwoording, met inachtneming van de toepasselijke privacywetgeving en het Uitvoeringsprotocol Social Return, praktisch kan worden ingericht. De Aanbestedende dienst doet in deze aanbestedingsfase geen toezegging over de acceptatie van specifieke alternatieve controlemethoden of bewijsstukken. Het Uitvoeringsprotocol Social Return blijft ongewijzigd van toepassing."

135	Uitvoeringsprotocol Social Return	Opdrachtgever stelt dat de invulling van de social return verplichting op enigerlei wijze verband moet houden met de inhoud van de opdracht. In verband met hooggeschoold en specialistisch werk, zowel binnen als in relatie tot de gegunde opdracht, is het niet altijd mogelijk om aan Social Return invulling te geven binnen de opdracht. Is het toegestaan om de Social Return verplichting binnen de bredere bedrijfsvoering van Opdrachtnemer in te vullen?	De Aanbestedende dienst bevestigt dit niet op voorhand. De Social Return-verplichting dient te worden ingevuld overeenkomstig het Uitvoeringsprotocol Social Return. De concrete en praktische invulling van deze verplichting wordt na gunning door Opdrachtnemer afgestemd met het Adviespunt Social Return. Indien invulling binnen de directe uitvoering van de opdracht niet of onvoldoende mogelijk blijkt, kan in dat overleg worden bezien welke andere vormen van invulling binnen de kaders van het Uitvoeringsprotocol passend en toegestaan zijn. Het Uitvoeringsprotocol Social Return blijft ongewijzigd van toepassing.
136	Paragraaf 3.2.1 Kerncompetentie 1	De aanbestedende dienst verlangt ervaring met het opzetten en beheren van een Microsoft Sentinel SIEM-oplossing voor een gemeentelijke organisatie van minimaal 420 gebruikers. Gezien de aard van de gevraagde dienstverlening zijn vergelijkbare eisen en complexiteit ook aanwezig bij andere overheidsorganisaties, zoals provincies, veiligheidsregio's, omgevingsdiensten, waterschappen en uitvoeringsorganisaties. Deze organisaties werken eveneens binnen de kaders van BIO, hybride ICT-infrastructuren en Microsoft-omgevingen. Kan de aanbestedende dienst bevestigen dat referenties van dergelijke overheidsorganisaties eveneens als passend bewijs voor Kerncompetentie 1 worden geaccepteerd, mits wordt voldaan aan de overige eisen ten aanzien van omvang, complexiteit en scope?	De opdrachtgever handhaaft voor Kerncompetentie 1 de eis dat de referentie betrekking heeft op een gemeentelijke organisatie. Een referentie van een provincie, veiligheidsregio, omgevingsdienst, waterschap of uitvoeringsorganisatie wordt daarom niet als vervanging voor deze gemeentelijke referentie geaccepteerd, ook niet als de organisatie volgens de inschrijver vergelijkbaar is qua omvang, hybride infrastructuur en beveiligingsvereisten. De opdrachtgever verlangt deze referentie omdat de ervaring moet aantonen dat de inschrijver de Microsoft Sentinel-oplossing heeft ingericht en beheerd binnen de gemeentelijke ICT-context, waaronder de voor gemeenten relevante organisatorische en wettelijke kaders. De overige voorwaarden, waaronder de vergelijkbare complexiteit, hybride ICT-infrastructuur en minimaal 420 gebruikers (60% van het totaal), blijven eveneens van toepassing. Dit sluit aan bij de eerdere beantwoording over Kerncompetentie 1: de aanbestedingsstukken vragen specifiek om gemeentelijke ervaring.
137	Paragraaf 3.2.1 Kerncompetentie 1 en Kerncompetentie 2	Kan de aanbestedende dienst bevestigen dat overal waar in de kerncompetenties de term gemeentelijke organisatie wordt gebruikt, gelezen mag worden overheidsorganisatie binnen de Nederlandse publieke sector, waaronder gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen en gemeenschappelijke regelingen? Hierdoor blijft de gevraagde ervaring inhoudelijk gelijkwaardig terwijl de mededinging wordt vergroot.	Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie.
138	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.2 en 2.22.	Kan Aanbestedende Dienst per in eis 2.2 genoemde logbron het huidige of geschatte dagelijkse datavolume in GB/dag, het aantal events per seconde waar beschikbaar, de gewenste retentieperiode en het aantal relevante assets en gebruikers opgeven? Indien deze informatie niet beschikbaar is, welke uitgangspunten dient Inschrijver hiervoor bij het technisch ontwerp, de capaciteitsbepaling en kostenoptimalisatie te hanteren?	In het prijzenblad worden kwantiteiten geplaatst voor gebruikersaantallen, werkplekken, servers en meer. Voor andere log-genererende apparatuur zoals firewalls switches etc. is momenteel geen logvolume bekend. Deze wordt echter grotendeels bepaald door de log-configuratie van deze apparaten. Hiervan verwacht de gemeente dat de dienstverlener aan kan geven welke log-configuratie een goed balans tussen relevante context en en verbruik is. Het aantal appliances wordt in het prijsblad opgenomen.
139	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.16 en 2.22 en hoofdstuk 5; Bijlage F1 - Prijzenblad SIEM SOC dd 08-10-2026.xlsx, jaarlijkse kosten logbronnen.	Zijn de Microsoft Azure- en Microsoft Sentinel-consumptiekosten onderdeel van de door Inschrijver aangeboden prijs, of worden deze rechtstreeks door Aanbestedende Dienst via haar bestaande Azure-overeenkomst gedragen en betreft de gevraagde prijs uitsluitend de SIEM/SOC-dienstverlening en het functionele en technische beheer daarvan?	De Microsoft Azure- en Microsoft Sentinel-consumptiekosten worden rechtstreeks door de opdrachtgever gedragen via de bestaande Azure-contract- en factureringsrelatie van de gemeente. Zij maken geen deel uit van de door de inschrijver aangeboden prijs voor SIEM/SOC-dienstverlening.

140	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.20 en 4.2; Bijlage F1 - Prijzenblad SIEM SOC dd 08-10-2026.xlsx, onderdeel 24x7x365 eyes on screen meerprijs ten opzichte van piketdienst.	Kan Aanbestedende Dienst bevestigen dat voor de vereiste 24/7 dienstverlening conform eisen 2.20 en 4.2 een piket- of consignatiemodel, ondersteund door automatisering, is toegestaan, mits alle overeengekomen triage-, analyse- en escalatietermijnen worden gehaald? Kan tevens worden bevestigd dat permanente 24x7x365 personele bezetting met “eyes on screen” uitsluitend als optionele dienstverlening wordt beschouwd, zoals opgenomen in het prijzenblad?	Ja. De verplichte basisdienstverlening moet voldoen aan de eisen voor 24/7-detectie, ontvangst en verwerking van beveiligingsmeldingen en voor 24/7-triage, analyse en zo nodig escalatie van kritieke en hoge meldingen (P1 en P2). De aanbestedingsstukken schrijven daarbij geen permanente personele bezetting voor. Een combinatie van geautomatiseerde bewaking en een 24/7 bereikbare piketdienst is toegestaan, mits aantoonbaar aan alle toepasselijke kwaliteits- en SLA-termijnen wordt voldaan. Ja. De post ‘24x7x365 eyes on screen meerprijs ten opzichte van piketdienst’ in Bijlage F1 betreft een optionele aanvullende dienst zonder afnameverplichting. Deze optie ziet op permanente personele bewaking van het scherm; zij is geen onderdeel van de verplichte basisdienst en vervangt de verplichting om de basisdienst 24/7 volgens de afgesproken normen te leveren niet. De inschrijver licht in zijn aanbieding toe hoe de basisdienst is ingericht en wat de meerwaarde en operationele invulling van de optionele eyes on screen-dienst is.
141	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.16, 2.19 en 4.19.	Beschikt Aanbestedende Dienst reeds over een bestaande Microsoft Sentinel-omgeving en bijbehorende Log Analytics-workspace of workspaces? Zo ja, kan inzicht worden gegeven in de huidige architectuur, configuratie, retentie, ingestievolumes, aangesloten databronnen, analytics rules, automation rules, playbooks, workbooks en eventuele eerder ontwikkelde maatwerkcomponenten?	Nee, Bij aanvang van deze aanbesteding zijn er geen bestaande sentinel omgevingen, of daarbij horende log analytics workspaces.
142	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eis 2.2; Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, § 5.1.1, subgunningscriterium B.	Kan Aanbestedende Dienst inzicht geven in de huidige Microsoft-architectuur en de aanwezige licenties, waaronder Microsoft 365, Microsoft Entra ID, Microsoft Defender for Endpoint, Defender for Servers, Defender for Identity en eventuele overige Microsoft Defender XDR-componenten, inclusief de toepasselijke licentieniveaus en aantallen?	Het prijzenblad zal worden bijgewerkt met daarin kwantificaties die relevant zijn voor de gevraagde componenten waar kwantificeerbaar.
143	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.2 en 2.13.	Kan Aanbestedende Dienst voor Cisco Duo, HelloID, Cisco Meraki, Barracuda, DNS, DHCP, SecureMe2 NIDS en Holm Security aangeven welke producten, versies en edities worden gebruikt en via welke interfaces de relevante loggegevens beschikbaar zijn, bijvoorbeeld syslog, CEF, API, Microsoft Event Hub of andere interfaces? Kan tevens worden aangegeven of de benodigde API- en exportlicenties reeds aanwezig zijn?	Zie antwoord vraag 120. Holm Security en SecureME2 maken gebruik van API.
144	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.2, 2.13 en 2.17.	Kan Aanbestedende Dienst aangeven hoeveel on-premises Active Directory Domain Controllers, DNS-servers en DHCP-servers binnen scope vallen, op welke platformen en versies deze draaien en of deze systemen reeds zijn voorzien van een mechanisme voor centrale logforwarding?	Het prijzenblad zal worden bijgewerkt met daarin kwantificaties die relevant zijn voor de gevraagde componenten waar kwantificeerbaar. Er zijn nog geen logforwarding mechanismen in-place.
145	Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, § 3.2.1; Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.2 en 2.20.	Kan Aanbestedende Dienst het actuele aantal gebruikers, endpoints, Windows-servers, overige servers, Domain Controllers en overige relevante assets binnen scope bevestigen, inclusief de verwachte groei of krimp gedurende de contractperiode?	Het prijzenblad zal worden bijgewerkt met daarin kwantificaties die relevant zijn voor de gevraagde componenten waar kwantificeerbaar. Er zijn nog geen logforwarding mechanismen in-place. Groei in de nabije toekomst is op dit moment lastig te voorspellen.

146	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eis 2.2.	In eis 2.2 wordt gesteld dat voor de genoemde logbronnen passende aanvullende use-cases “out of the box” moeten worden ondersteund. Kan Aanbestedende Dienst verduidelijken wat zij onder “out of the box” verstaat? Worden hieronder ook standaard Microsoft Sentinel Content Hub-oplossingen, Microsoft Defender XDR-detecties en reeds door Opdrachtnemer ontwikkelde generieke detectiecontent verstaan die voor de omgeving van Opdrachtgever wordt geconfigureerd?	Met “out of the box” bedoelt de opdrachtgever dat voor de in eis 2.2 genoemde logbronnen passende aanvullende use-cases beschikbaar zijn zonder dat daarvoor eerst geheel nieuwe detectiecontent hoeft te worden ontwikkeld. Dit omvat bestaande standaardcontent van Microsoft Sentinel, waaronder relevante oplossingen en detectieregels uit de Content Hub, Microsoft Defender XDR-detecties en reeds door de opdrachtnemer ontwikkelde generieke detectiecontent.
147	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.19 en 4.19.	Eis 2.19 vraagt om een koppeling tussen Microsoft Sentinel en het SOC voor registratie en actualisering van incidenten, terwijl eis 4.19 Microsoft Sentinel benoemt als centraal platform voor monitoring, correlatie, onderzoek en incidentregistratie. Kan Aanbestedende Dienst verduidelijken of Microsoft Sentinel de primaire incidentregistratie dient te zijn, of dat een bidirectionele koppeling met een afzonderlijk SOC-, ITSM- of ticketsysteem wordt verwacht?	Ja. Microsoft Sentinel binnen de Microsoft-tenant van de opdrachtgever is het primaire centrale platform voor beveiligingsmonitoring, correlatie, onderzoek en incidentregistratie, zoals bepaald in eis 4.19. Eis 2.19 verlangt daarnaast een koppeling tussen Sentinel en het SOC, zodat relevante incidentgegevens en statusinformatie tussen beide omgevingen kunnen worden geregistreerd en bijgewerkt. De aanbestedingsstukken verplichten niet tot een afzonderlijk SOC-, ITSM- of ticketsysteem. Als de opdrachtnemer zo’n systeem gebruikt, moet de koppeling met Sentinel de registratie en actualisering van relevante incidentgegevens ondersteunen. De precieze gegevensuitwisseling en statussynchronisatie worden tijdens de implementatie met de opdrachtgever vastgesteld. Aanvullende tooling mag worden ingezet als die aantoonbare meerwaarde biedt en geen afbreuk doet aan de toegang, zeggenschap, beveiliging, prestaties, overdraagbaarheid of gegevensbescherming van de opdrachtgever.
148	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 4.7 en 4.19.	Eis 4.7 vereist registratie van incidenten in een voor de gemeente toegankelijk portal. Is het voldoende wanneer deze informatie rechtstreeks via Microsoft Sentinel beschikbaar is, eventueel aangevuld met het bestaande klantportaal van Opdrachtnemer, of wordt een afzonderlijk ITSM- of incidentmanagementplatform vereist? Indien een afzonderlijk platform wordt vereist, welke functionele eisen gelden hiervoor?	Er is geen afzonderlijk ITSM- of incidentmanagementplatform voorgeschreven. Microsoft Sentinel binnen de tenant van de opdrachtgever is het centrale platform voor monitoring, onderzoek en incidentregistratie (eis 4.19). Incidentinformatie moet daarin rechtstreeks voor de gemeente toegankelijk zijn en voldoen aan de registratievereisten van eis 4.7.
149	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 4.17, 6.8 en 6.9; Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, § 5.1.1, subgunningscriterium B, onderdeel SOAR.	Welke geautomatiseerde responsacties wenst Aanbestedende Dienst bij aanvang van de dienstverlening vooraf te mandateren? Kan tevens worden aangegeven voor welke systemen, bedrijfskritische processen of typen incidenten uitsluitend human approval is toegestaan voordat een responseactie wordt uitgevoerd?	De aanbestedingsstukken verlangen dat de opdrachtnemer een voorstel doet voor de inzet van SOAR, waaronder automatiseringsprocessen, use-cases, playbooks en de kwaliteitsborging daarvan. Zij wijzen echter geen specifieke responsacties aan die de gemeente bij aanvang al vooraf mandateert, en bepalen evenmin voor welke systemen, processen of incidenttypen altijd voorafgaande menselijke goedkeuring vereist is. Responsacties in de gemeentelijke omgeving mogen uitsluitend worden uitgevoerd binnen bevoegdheden en mandaten die vooraf expliciet en schriftelijk zijn vastgelegd, bijvoorbeeld per actie of use-case in het DAP en de playbooks. Zonder zo’n mandaat is voorafgaande beoordeling en besluitvorming door de opdrachtgever vereist. Dit geldt ook voor ingrijpende acties zoals het isoleren van hosts, blokkeren van netwerkverkeer of intrekken van accounts. Eis 6.9 bepaalt dat uitkomsten van AI, machine learning of andere geautomatiseerde analyses vóór escalatie of uitvoering van een responsactie door een gekwalificeerde medewerker worden beoordeeld, tenzij voor de betreffende actie vooraf schriftelijk mandaat is verleend. De gemeente stelt eventuele mandaten en vereisten voor menselijke goedkeuring tijdens de implementatie vast; de inschrijver beschrijft in zijn inschrijving hoe hij dit proces en de bijbehorende waarborgen inricht.

150	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.1, 2.32 en 3.3.	Kan Aanbestedende Dienst voor UC1 tot en met UC5 aangeven welke minimale detectiescenario's, analytics rules, responseacties en acceptatiecriteria gelden om een use-case als geïmplementeerd en geaccepteerd te beschouwen? Is het aan Inschrijver om binnen de beschreven doelstellingen zelf passende detectiescenario's en regels te definiëren?	De opdrachtgever verstrekt geen vooraf vastgestelde, uitputtende lijst van verplichte detectiescenario's, analytics rules, responsacties of numerieke acceptatiegrenswaarden voor UC1 tot en met UC5. De use-cases in eis 2.1 beschrijven de te bereiken detectiedoelen. Het is aan de inschrijver om binnen die doelen passende detectiescenario's en regels voor te stellen en in de inschrijving inzichtelijk te maken. Tijdens de implementatie werken opdrachtnemer en opdrachtgever de use-cases samen uit. Per use-case worden de relevante scenario's, beschikbare logbronnen, detectielogica, testaanpak en concrete acceptatiecriteria vastgelegd. De opdrachtnemer implementeert, test en documenteert de vijf use-cases. De opdrachtgever accepteert deze bij de initiële oplevering overeenkomstig eis 3.3. Klantspecifieke use-cases worden uitsluitend na de overeengekomen test en autorisatie in productie genomen, zoals bepaald in eis 2.32.
151	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eis 2.18.	Verwacht Aanbestedende Dienst dat Inschrijver tijdens de implementatie een formele MITRE ATT&CK coverage assessment en mapping oplevert? Zo ja, wordt hiervoor een specifieke minimale dekking, volwassenheidsniveau of rapportagevorm verwacht?	Nee. Eis 2.18 vraagt dat Opdrachtnemer detectie uitvoert op basis van actuele aanvalstechnieken, zoals onder andere beschreven in het MITRE ATT&CK framework. De eis vraagt niet dat Opdrachtnemer dit tijdens de implementatie aantoont met een formele coverage assessment of mapping. Er geldt daarom geen minimale dekkingsgraad, volwassenheidsniveau of voorgeschreven rapportagevorm. Wel verwacht Aanbestedende Dienst dat de aangesloten logbronnen worden benut voor detectie op relevante aanvalstechnieken. Opdrachtnemer kan daarbij naar eigen inzicht gebruikmaken van het MITRE ATT&CK framework.
152	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.22, 5.5 en 8.4.	Welke minimale online- en archiefretentieperiode verlangt Aanbestedende Dienst voor de verschillende categorieën SIEM-loggegevens en securitydata? Kunnen deze perioden per logbron verschillen op basis van detectiewaarde, onderzoeksbehoefte, wettelijke bewaartermijnen, privacy en kosten?	Eis DIV31 stelt een maximale bewaartermijn van één jaar na vastlegging voor SIEM-logdata en SOC-rapportagedata. De aangeleverde stukken leggen geen algemene bewaartermijn vast voor alle overige gegevens, waaronder incidentdossiers, onderzoeksgegevens, bewijslast, IoC's, incidentmetadata, detectieregels, configuraties en gegevens in Microsoft Sentinel.
153	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.22 en 6.6.	Staat Aanbestedende Dienst toe dat Opdrachtnemer, na afstemming en goedkeuring door Opdrachtgever, filtering en transformatie toepast vóór of tijdens ingestie in Microsoft Sentinel, bijvoorbeeld via Azure Monitor Data Collection Rules, wanneer gegevens aantoonbaar geen relevante detectie-, onderzoeks-, audit- of compliancewaarde hebben?	Ja, filtering en transformatie van logdata vóór of tijdens ingestie in Microsoft Sentinel, bijvoorbeeld via Azure Monitor Data Collection Rules, is toegestaan na voorafgaande afstemming en schriftelijke goedkeuring van de opdrachtgever.
154	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.16, 2.17, 2.18 en 4.19; Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, § 5.1.1, subgunningscriterium B.	Is het toegestaan en gewenst dat Microsoft Defender XDR, voor zover ondersteund door de aanwezige licenties, wordt ingezet als integraal onderdeel van de detectie- en responseketen, waarbij Microsoft Sentinel fungeert als centraal SIEM-platform voor cross-domain correlatie, aanvullend onderzoek, incidentregie en SOC-monitoring?	Ja, de opdrachtgever staat toe dat Microsoft Defender XDR, voor zover de gemeente over de benodigde licenties beschikt en de functionaliteit binnen de gemeentelijke tenant is ingericht, wordt ingezet als onderdeel van de detectie- en responseketen.

155	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eis 4.12; Bijlage F1 - Prijzenblad SIEM SOC dd 08-10-2026.xlsx, onderdeel CERT-dienstverlening en IR Retainers.	Kan Aanbestedende Dienst verduidelijken waar de grens ligt tussen reguliere SOC-incidentanalyse en specialistische Incident Response- of CERT-dienstverlening? Welke activiteiten bij een critical incident worden geacht onderdeel te zijn van de reguliere dienstverlening en vanaf welk moment geldt de optionele CERT- of IR-dienstverlening uit het prijzenblad?	De reguliere SOC-dienstverlening is erop gericht vast te stellen dat sprake is van een beveiligingsincident of een zich ontwikkelend incident, en Opdrachtgever tijdig in staat te stellen daarop te handelen. Dit omvat bij alle incidenten, ook kritieke incidenten, ten minste: 24/7 monitoring, detectie, triage, analyse, classificatie, melding en escalatie (eisen 2.20, 4.2 en 4.17); registratie van het incident conform eis 4.7; het uitvoeren van vooraf gemandateerde responsacties ten behoeve van isolatie en eerste herstel (eis 4.17 en bijlage 9.2); een eerste bruikbare analyse en advies over vervolg- en mitigerende maatregelen (eis 8.14). Wanneer een incident een respons vereist die verder gaat dan de vooraf vastgelegde mandaten, escaleert Opdrachtnemer naar Opdrachtgever. Opdrachtgever beschikt op dit moment over een IR-retainer bij een andere partij en schaalt in eerste instantie daarmee op. Van Opdrachtnemer wordt dan verwacht dat hij, vanuit zijn informatiepositie, de ingrijpende partij ondersteunt en faciliteert. Dat betekent onder meer het delen van analyses, tijdlijnen, bewijslast en IOC's, het uitvoeren van aanvullende zoekopdrachten en het monitoren op hernieuwde activiteit (zie ook eisen 2.12 en 4.12). Deze ondersteuning maakt deel uit van de reguliere dienstverlening. De in het Prijzenblad opgenomen CERT/IR-dienstverlening is een optionele prijscomponent zonder afnameverplichting. Deze wordt uitsluitend ingezet na expliciete opdracht van Opdrachtgever.
156	Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, § 3.2.1, Kerncompetentie 2, onderdeel root-causeanalyse; Bijlage E - Document Bewijsstuk referentie.docx, Kerncompetentie 2.	Welke diepgang wordt verwacht van root-causeanalyses binnen de reguliere SOC-dienstverlening? Betreft dit een technische analyse op basis van de binnen het SIEM- en XDR-platform beschikbare telemetrie, of wordt ook volledige digitale forensics op endpoints, servers, identity-systemen en netwerkcomponenten verwacht?	Binnen de reguliere SOC-dienstverlening wordt een technische analyse verwacht op basis van de telemetrie die beschikbaar is in Microsoft Sentinel, de Microsoft Defender-producten en de overige aangesloten logbronnen. Deze analyse moet voldoende diepgang hebben om vast te stellen of sprake is van een (zich ontwikkelend) incident, wat de vermoedelijke oorzaak en aanvalsroute zijn en welke identiteiten en assets betrokken zijn. Op basis daarvan geeft Opdrachtnemer onderbouwd advies over escalatie en mitigerende maatregelen. Volledige digitale forensics op endpoints, servers, identity-systemen en netwerkcomponenten valt niet onder de reguliere dienstverlening. Indien dit noodzakelijk is, wordt dit uitgevoerd door de door Opdrachtgever ingeschakelde incident response-partij, waarbij Opdrachtnemer ondersteunt zoals beschreven in het antwoord op vraag 155.
157	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 2.15, 2.21 en 3.5.	Kan Aanbestedende Dienst bevestigen dat vóór aanvang van de implementatie een actuele netwerktekening, Microsoft tenant- en Azure-architectuur, identity-architectuur, overzicht van securitytooling, asset inventory en overzicht van relevante datastromen aan Opdrachtnemer beschikbaar worden gesteld? Indien onderdelen niet beschikbaar zijn, wordt van Opdrachtnemer verwacht dat deze binnen de vaste implementatieprijs worden opgesteld?	Opdrachtgever stelt bij aanvang van de implementatie de beschikbare documentatie ter beschikking. Opdrachtgever kan niet garanderen dat alle in de vraag genoemde documentatie volledig en actueel beschikbaar is. Van Opdrachtnemer wordt niet verwacht dat hij ontbrekende architectuurdocumentatie van de gemeentelijke omgeving integraal opstelt. Wel wordt verwacht dat Opdrachtnemer de informatie verzamelt die nodig is voor de ontwerpen uit eisen 2.15 en 2.21, voor zover relevant voor de SIEM/SOC-oplossing. Deze werkzaamheden vallen binnen de vaste implementatieprijs. Opdrachtgever en de betrokken IT-dienstverlener(s) verlenen hieraan medewerking, zoals ook volgt uit eisen 3.3 en 3.5.

158	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eisen 5.6 en 5.7.	In eis 5.6 wordt een implementatiescope beschreven die onder meer bestaat uit projectmanagement, ontwerp, inrichting en configuratie van Microsoft Sentinel, aansluiting van de overeengekomen initiële logbronnen, implementatie en acceptatie van vijf initiële use-cases, SOC-inrichting, documentatie, opleiding, testen, herstel van bevindingen en ondersteuning tijdens de stabilisatieperiode. Eis 5.7 maximeert de implementatiekosten op €15.000. Kan Aanbestedende Dienst bevestigen dat alle in eis 5.6 beschreven activiteiten volledig binnen dit maximumbedrag moeten worden uitgevoerd? Zo ja, kan zij verduidelijken welke uitgangspunten ten aanzien van aantallen logbronnen, connectorcomplexiteit, inzet van derden, testen en acceptatiewerkzaamheden aan dit maximumbedrag ten grondslag liggen?	Ja. De opdrachtgever bevestigt dat alle in eis 5.6 genoemde activiteiten volledig binnen het maximum van € 15.000 aan totale implementatiekosten moeten worden uitgevoerd. Het betreft een vaste prijs voor de werkzaamheden die nodig zijn om de overeengekomen initiële implementatiescope volledig, werkend en geaccepteerd op te leveren. De opdrachtgever heroverweegt dit maximum niet. Het prijzenblad vraagt om één totaalprijs voor ontwerp en implementatie van de volledige scope. De stukken geven geen afzonderlijke vaste aantallen op voor alle logbronnen of voor de benodigde inzet van derden. Zoals eerder toegelicht, vullen inschrijvers de aantallen en eenheden bij de logbronnen in op basis van hun eigen, expliciet toegelichte aannames. Bij de implementatie omvat de vaste prijs in ieder geval het aansluiten van de overeengekomen essentiële logbronnen en het implementeren, testen, documenteren en laten accepteren van de vijf initiële use-cases. Ook de noodzakelijke projectleiding, opleiding, herstel van bevindingen en stabilisatieondersteuning vallen binnen dit bedrag.
159	Bijlage A - Programma van Eisen SIEM SOC dd 08-10-2026.pdf, eis 5.1; Aanbestedingsdocument SIEM SOC dd 08-10-2026.pdf, §§ 1.1.3 en 5.1.2.	In eis 5.1 van het Programma van Eisen wordt gesproken over een initiële contractduur van vier jaar. In §1.1.3 van het Aanbestedingsdocument wordt echter een vaste looptijd van drie jaar genoemd, gevolgd door drie verlengingsopties van ieder twee jaar. Kan Aanbestedende Dienst bevestigen dat de vaste contractduur drie jaar bedraagt en dat de verwijzing naar vier jaar in eis 5.1 als een kennelijke verschrijving moet worden beschouwd?	Correct, dit is inderdaad een verschrijving in eis 5.1 van het PvE. De nieuw af te sluiten overeenkomst kent, na de implementatieperiode, een vaste looptijd van drie (3) jaar en heeft een beoogde startdatum van 1 maart 2027. Na deze vaste looptijd kan de overeenkomst drie (3) maal met een periode van telkens twee (2) jaar worden verlengd. De maximale looptijd van de overeenkomst bedraagt daarmee maximaal negen (9) jaar.
160	Aanbestedingsdocument §3.2.1 – Technische bekwaamheid en beroepsbekwaamheid, Kerncompetentie 1 en 2	Kan de aanbestedende dienst bevestigen of voor het aantonen van de genoemde kerncompetenties ook referentieopdrachten bij andere organisaties mogen worden gebruikt, indien aard, omvang en complexiteit van de uitgevoerde SIEM/SOC-dienstverlening aantoonbaar vergelijkbaar of groter zijn dan de gevraagde dienstverlening?	Nee, aanbestedende dienst is (enkel) op zoek naar partijen die over een kerncompetentie beschikken voor een gemeentelijke organisatie met tenminste 420 gebruikers. De gemeente Vijfheerenlanden is een organisatie met ongeveer 700 gebruikers. De 420 gebruikers (60% van het totaal) is daarmee de ondergrens van gebruikers.
161	Aanbestedingsdocument §3.2.1 – Technische bekwaamheid en beroepsbekwaamheid, Kerncompetentie 1 en 2	Indien vergelijkbare referentieopdrachten bij andere organisaties zijn toegestaan, mogen hiervoor ook referentieopdrachten buiten Nederland worden gebruikt?	Nee dat is niet toegestaan

162	Programma van Eisen 2.2 en 5.5 / Prijzenblad F1	Kan de aanbestedende dienst voor de genoemde logbronnen de verwachte aantallen assets/accounts en, waar beschikbaar, het huidige of verwachte dagelijkse datavolume (GB/dag) en de gewenste retentie verstrekken, zodat inschrijvers de dienstverlening en bijbehorende kosten op een uniforme basis kunnen calculeren?	De verwachte aantallen gebruikers, assets en devices per logbron, zoals accounts, endpoints, servers en firewalls, worden opgenomen in het geactualiseerde Prijzenblad dat bij deze Nota van Inlichtingen wordt gepubliceerd. Aanbestedende Dienst beschikt niet over betrouwbare gegevens over het huidige of verwachte dagelijkse datavolume per logbron. Voor prijscomponenten die afhankelijk zijn van datavolume vermeldt Inschrijver conform eis 5.5 de gehanteerde eenheid, het tarief en de onderliggende aannames. Van Opdrachtnemer wordt verwacht dat hij Opdrachtgever adviseert over een passende balans tussen detectiewaarde en datavolume en de daarmee samenhangende kosten. Dit geldt zowel tijdens de implementatie als gedurende de looptijd (eisen 2.22 en 4.18). Daarbij hoort ook advies over welke gegevens per logbron worden ingelezen en over eventuele filtering. De retentie van loggegevens in Microsoft Sentinel bedraagt twaalf maanden. De Azure-verbruikskosten van Microsoft Sentinel, waaronder kosten voor data-inname en retentie, worden rechtstreeks door Opdrachtgever afgerekend en maken geen onderdeel uit van de inschrijvingsprijs.
163	Aanbestedingsdocument SIEM SOC, paragraaf 5.1.1	Kan Aanbestedende Dienst verduidelijken hoe wordt geborgd dat gunningscriterium D (Demonstratie) uitsluitend een verificatie vormt van de schriftelijke inschrijving, nu dit criterium tevens zelfstandig wordt beoordeeld? Welke beoordelingsaspecten mogen tijdens de demonstratie nog tot scoreverschillen leiden en op welke wijze wordt voorkomen dat nieuwe informatie, niet opgenomen in de schriftelijke inschrijving, alsnog wordt meegewogen in de gunning?	De Aanbestedende dienst verduidelijkt dat gunningscriterium D (Demonstratie) geen uitsluitend verificatief karakter heeft, maar een zelfstandig gunningscriterium vormt. De demonstratie wordt beoordeeld aan de hand van de voor gunningscriterium D in de aanbestedingsstukken opgenomen beoordelingsaspecten en leidt tot een afzonderlijk eindcijfer. (zie ook vraag en antwoord 78) Tijdens de demonstratie mag de Inschrijver de aangeboden oplossing en werkwijze toelichten en demonstreren. De daarbij verstrekte informatie mag echter niet leiden tot een wijziging van de Inschrijving of tot herstel dan wel aanvulling van hetgeen op grond van de aanbestedingsstukken reeds bij Inschrijving had moeten zijn aangeboden of aangetoond. Scoreverschillen voor gunningscriterium D kunnen uitsluitend voortvloeien uit de mate waarin tijdens de demonstratie wordt voldaan aan de voor dit criterium vooraf bekendgemaakte beoordelingsaspecten. De demonstratieaspecten worden integraal en in onderlinge samenhang beoordeeld en leiden tot één eindcijfer. Er worden geen andere of niet vooraf bekendgemaakte beoordelingsaspecten meegewogen.
164	Aanbestedingsdocument SIEM SOC, paragraaf 5.1.1	In paragraaf 5.1.1 (gunningscriterium D) wordt aangegeven dat de demonstratie een uitwerking omvat van minimaal één use case naar keuze van de Inschrijver. Kan Aanbestedende Dienst bevestigen dat iedere Inschrijver volledig vrij is in de keuze van deze use case? Indien dit het geval is, kan Aanbestedende Dienst toelichten op welke wijze een objectieve en onderling vergelijkbare beoordeling wordt geborgd, nu verschillende use cases kunnen verschillen in aard, scope, complexiteit en demonstrabele functionaliteit?	Ja. Iedere Inschrijver is vrij in de keuze van de te demonstreren use case, met inachtneming van hetgeen hierover bij gunningscriterium D is bepaald. De onderlinge vergelijkbaarheid wordt geborgd doordat niet de aard of complexiteit van de gekozen use case als zodanig wordt beoordeeld, maar de wijze waarop de Inschrijver aan de hand daarvan invulling geeft aan de vooraf bekendgemaakte beoordelingsaspecten van gunningscriterium D. Voor alle Inschrijvers geldt hetzelfde beoordelingskader en dezelfde beoordelingssystematiek. De keuze voor een meer of minder complexe use case levert als zodanig geen hogere of lagere waardering op. De beoordelingsaspecten worden integraal en in onderlinge samenhang beoordeeld en leiden tot één eindcijfer voor de demonstratie.
165	Aanbestedingsdocument SIEM SOC, paragraaf 5.2.2	Kan Aanbestedende Dienst bevestigen dat uitsluitend toegevoegde waarde die aantoonbaar bijdraagt aan de in de aanbestedingsstukken beschreven doelstellingen, behoeften en beoordelingscriteria positief wordt gewaardeerd? Met andere woorden: leidt additionele, maar niet uitgevraagde functionaliteit of dienstverlening op zichzelf tot een hogere score, of uitsluitend indien deze rechtstreeks aansluit op de gepubliceerde beoordelingscriteria?	Additionele functionaliteit of dienstverlening leidt niet op zichzelf tot een hogere waardering. Toegevoegde waarde wordt uitsluitend positief gewaardeerd voor zover deze relevant is voor en aantoonbaar bijdraagt aan de doelstellingen en beoordelingsaspecten zoals opgenomen bij het betreffende gunningscriterium. Functionaliteit of dienstverlening die geen relevante relatie heeft met de vooraf bekendgemaakte beoordelingsaspecten, wordt niet als zelfstandige meerwaarde in de beoordeling betrokken. De gepubliceerde gunnings- en beoordelingssystematiek blijft ongewijzigd van toepassing.

166	Aanbestedingsdocument SIEM SOC, algemeen	Kan Opdrachtgever bevestigen dat de scope van deze opdracht uitsluitend betrekking heeft op de in de aanbestedingsstukken genoemde IT-omgevingen en logbronnen, en dat OT-, ICS- of andere vitale infrastructuuromgevingen (zoals bruggen, sluizen, verkeersregelinstallaties en gemalen) geen onderdeel uitmaken van de gevraagde dienstverlening? Indien dit niet het geval is, verzoekt Inschrijver om een nadere specificatie van de betreffende objecten, systemen en beveiligingsvereisten.	De opdracht betreft de SIEM/SOC-dienstverlening en de logbronnen zoals omschreven in de aanbestedingsstukken, waaronder de veertien bronnen in eis 2.2. De stukken sluiten andere relevante logbronnen, systemen of beveiligingsoplossingen niet categorisch uit. De opsomming in eis 2.2 is daarom niet zonder meer een uitputtende afbakening van alle bronnen die gedurende de overeenkomst kunnen worden aangesloten.
167	Aanbestedingsdocument SIEM SOC, algemeen	Inschrijver begrijpt uit de aanbestedingsstukken dat bij de uitvoering van de opdracht mogelijk sprake is van samenwerking met externe IT-dienstverleners, leveranciers en andere betrokken derden. Kan Opdrachtgever aangeven in hoeverre de ICT-infrastructuur en beveiligingsomgeving in eigen beheer worden uitgevoerd en voor welke onderdelen gebruik wordt gemaakt van derde partijen? Indien hiervan sprake is, verzoekt Inschrijver een overzicht te verstrekken van de betrokken partijen, hun rol en verantwoordelijkheden, alsmede de mate waarin Opdrachtnemer voor implementatie, beheer, wijzigingsprocessen en incidentafhandeling afhankelijk is van hun medewerking.	De documenten maken onderscheid tussen de inventarisatie en coördinatie van betrokken partijen en een vooraf volledig overzicht van die partijen. Ze verplichten niet tot het bij de inschrijving verstrekken van een uitputtende lijst van alle interne en externe ICT-dienstverleners, hun contracten en onderlinge afhankelijkheden.
168	Aanbestedingsdocument SIEM SOC, algemeen	Kan Opdrachtgever aangeven of momenteel sprake is van externe dienstverlening op het gebied van monitoring, SOC, MDR, incidentdetectie en/of incidentafhandeling? Indien hiervan sprake is, verzoekt Inschrijver te verduidelijken welke onderdelen van de dienstverlening reeds zijn ingericht, welke kennis, detectieregels, use-cases, procedures en historische informatie beschikbaar zijn voor overdracht, en welke transitieverplichtingen van een nieuwe Opdrachtnemer worden verwacht.	Nee, er is op dit moment geen sprake van externe dienstverlening.
169	Aanbestedingsdocument SIEM SOC, algemeen	Kan Opdrachtgever aangeven of zij op basis van haar huidige Microsoft-licenties beschikt over het recht om Microsoft Defender Vulnerability Management (MDVM) te gebruiken? Indien dit het geval is, verzoekt Inschrijver te verduidelijken of Opdrachtgever reeds gebruik maakt van MDVM of voornemens is dit gedurende de looptijd van de overeenkomst te gaan inzetten.	Wordt op dit moment niet gebruikt, ondanks dat door M365 E5 de nodige licenties al aanwezig kunnen zijn. Binnen de gemeente wordt gebruik gemaakt van HOLM Security voor het beheeren van de kwetsbaarheden.
170	Bijlage A, Eis 7.6	Kan Aanbestedende Dienst verduidelijken welke concrete eisen zij stelt aan eis 7.6 ten aanzien van overdraagbaarheid? Wanneer is daaraan voldaan?	Eis 7.6 is een functionele eis. De dienstverlening moet zo worden ingericht dat de gemeente deze bij afloop of beëindiging van de overeenkomst zelf, of met een opvolgende leverancier, kan voortzetten zonder onnodige afhankelijkheid van de zittende opdrachtnemer. Daaraan is voldaan wanneer de gemeente gedurende de overeenkomst rechtstreeks toegang heeft tot de gemeentelijke gegevens en klantspecifieke configuraties, en de voor beheer en overdracht benodigde documentatie, koppelingen, use-cases, detectieregels, playbooks, rapportages en kennis tijdig en in een gangbaar, bruikbaar formaat beschikbaar krijgt. De overdracht en de daarvoor benodigde acties worden uitgewerkt en actueel gehouden in het Exitplan, overeenkomstig eisen 7.2 tot en met 7.5.

171	Bijlage A, Eis 7.7	Ten aanzien van eis 7.7 verzoekt Inschrijver Aanbestedende Dienst te verduidelijken welke werkzaamheden zij rekent tot de "reguliere exitwerkzaamheden" die geacht worden in de aangeboden prijzen te zijn inbegrepen. Kan Aanbestedende Dienst daarbij aangeven welke activiteiten, inspanningen en overdrachtswerkzaamheden ten minste onder deze verplichting vallen en welke werkzaamheden als aanvullende werkzaamheden worden beschouwd? Tevens verzoekt Inschrijver te bevestigen dat de exitbepalingen en kostenregeling uit de GIBIT 2025 onverkort van toepassing blijven op de overeenkomst.	Eis 7.7 blijft van toepassing: reguliere exitwerkzaamheden zijn inbegrepen in de aangeboden prijzen. Dit omvat in ieder geval het actueel houden en regulier uitvoeren van het Exitplan, de voorbereiding en planning van de overdracht, het opleveren van een actueel overzicht van overdrachtsrelevante gegevens en onderdelen, overdracht van gemeentelijke gegevens en configuraties in een gangbaar en bruikbaar formaat, overdracht van documentatie en kennis, overdracht van openstaande incidenten, en het intrekken van toegangen en verwijderen van gemeentelijke gegevens na schriftelijke acceptatie van de overdracht. Ook de in Bijlage A1 voorgeschreven gezamenlijke test van het Exitplan valt binnen de vaste prijs. De stukken schrijven daarvoor geen afzonderlijke vaste ureninzet of testfrequentie voor; de test wordt uitgewerkt in het Exitplan. Aanvullend migratie- of transitiewerk dat aantoonbaar buiten deze reguliere exitverplichtingen en de overeengekomen scope valt, kan uitsluitend na voorafgaande schriftelijke opdracht als meerwerk worden uitgevoerd. De opdrachtnemer moet de omvang en kosten vooraf specificeren. De GIBIT 2025 blijft van toepassing, maar de specifieke afspraken in de aanbestedingsstukken over inbegrepen reguliere exitwerkzaamheden gelden daarnaast. Voor werkzaamheden die daarbuiten vallen, gelden de GIBIT en de overeenkomst, met inachtneming van de daarin vastgelegde opdracht- en vergoedingsafspraken.
172	Bijlage A, Eisen 6.2, 6.3 en 7.2	Kan Aanbestedende Dienst bevestigen dat onder de eisen 6.3 en 6.4 uitsluitend die instellingen, configuraties, detectieregels, queries, use-cases en playbooks worden verstaan die specifiek voor Opdrachtgever zijn ontwikkeld, en dat generieke detectielogica, standaard use-cases, correlatieregels, playbooks, querybibliotheken, methodieken, templates, knowhow en overige intellectuele eigendomsrechten van Opdrachtnemer daarvan zijn uitgezonderd? Kan Aanbestedende Dienst tevens bevestigen dat de toegang tot de versiehistorie uitsluitend betrekking heeft op klantspecifieke wijzigingen en niet op de onderliggende generieke ontwikkelhistorie, methodieken of andere vertrouwelijke bedrijfsinformatie van Opdrachtnemer? De gevraagde eigendoms- en transparantieverplichtingen zijn in hun huidige formulering zeer ruim en kunnen ertoe leiden dat generieke MDR/SOC-componenten van Inschrijver, waarin aanzienlijke investeringen in ontwikkeling, threat intelligence en optimalisatie zijn gedaan, feitelijk aan derden beschikbaar moeten worden gesteld. Deze componenten vormen een essentieel onderdeel van het intellectueel eigendom en het bedrijfsdebiet van Opdrachtnemer en worden veelal voor meerdere klanten ingezet. Voor het voorkomen van vendor lock-in en het waarborgen van continuïteit is het voldoende dat de Aanbestedende Dienst toegang heeft tot de actuele, voor haar omgeving ingerichte configuraties, detectieregels en documentatie. Toegang tot generieke detectielogica en de volledige ontwikkel- en versiehistorie gaat verder dan noodzakelijk is	Ja, dat bevestigen wij. Eisen 6.3 en 6.4 gaan alleen over de instellingen, configuraties, detectieregels, queries, use cases en playbooks die specifiek voor de gemeente zijn ontwikkeld of ingericht. Generieke detectielogica, standaard use cases, correlatieregels, playbooks, querybibliotheken, methodieken, templates, knowhow en andere intellectuele eigendomsrechten van de opdrachtnemer blijven van de opdrachtnemer. Ook de toegang tot de versiehistorie geldt alleen voor de klantspecifieke wijzigingen in de omgeving van de gemeente, niet voor de generieke ontwikkelhistorie of andere vertrouwelijke bedrijfsinformatie van de opdrachtnemer. De gemeente moet wel altijd toegang hebben tot de actuele configuraties, detectieregels en documentatie van haar eigen omgeving, zodat de continuïteit gewaarborgd blijft.

173	Art 14.1 GIBIT 2025	Inschrijver stelt voor dat "menselijk toezicht" voor geautomatiseerde response-acties gezien de aard van de dienstverlening wordt ingevuld als (i) mogelijkheid tot achteraf-audit van elke geautomatiseerde actie, (ii) configureerbare drempelwaarden voor autonome actie overeengekomen in de SLA, en (iii) een eventuele escalatieprocedure. De praktijk van de MDR/SOC-dienstverlening is namelijk dat er binnen vooraf afgestemde kaders steeds meer zal worden toegewerkt naar geautomatiseerde response (bijv. automatische isolatie van een endpoint door SOAR). Menselijk toezicht vóóraf is dan operationeel onhaalbaar. Kan Aanbestedende DIenst hiermee instemmen?	De Aanbestedende dienst bevestigt dat artikel 14.1 GIBIT 2025 niet vereist dat aan iedere geautomatiseerde responsactie steeds vooraf een afzonderlijke menselijke goedkeuring voorafgaat. Geautomatiseerde responsacties zijn toegestaan voor zover deze plaatsvinden binnen vooraf met de Aanbestedende dienst schriftelijk vastgelegde bevoegdheden, mandaten en kaders. De inrichting dient daarbij passende mogelijkheden voor menselijk toezicht te bevatten, waaronder waar relevant controleerbare logging en audit achteraf, vooraf configureerbare voorwaarden en drempelwaarden en passende mogelijkheden voor interventie en escalatie. De concrete inrichting wordt afgestemd op de aard, impact en risico's van de betreffende geautomatiseerde responsactie en nader vastgelegd in de daarvoor bestemde operationele afspraken. Artikel 14 GIBIT 2025 en de eisen uit het Programma van Eisen blijven ongewijzigd van toepassing.
174	Art 14.4 GIBIT 2025	Inschrijver stelt voorop dat de interpretatie van de AI-verordening nog in ontwikkeling is (er is nog nauwelijks jurisprudentie). Op basis van eigen beoordelingen komt Inschrijver tot de conclusie dat door haar gehanteerde AI-systemen geen hoog risico zijn. Deze conclusie kan echter in de toekomst veranderen op basis van gewijzigde inzichten en ontwikkelingen in wetgeving en jurisprudentie. Kan daarom worden toegevoegd dat een gewijzigde classificatie achteraf binnen redelijke termijn door Leverancier moet worden gemeld?	De Aanbestedende dienst ziet geen aanleiding de GIBIT 2025 op dit punt aan te passen. Indien gedurende de looptijd van de Overeenkomst de toepasselijke classificatie van een binnen de dienstverlening gebruikt AI-systeem wijzigt of Opdrachtnemer redelijkerwijs behoort te voorzien dat deze wijzigt, dient Opdrachtnemer de Aanbestedende dienst hierover tijdig te informeren en inzicht te geven in de gevolgen daarvan voor de dienstverlening en de toepasselijke verplichtingen. Partijen dienen gedurende de looptijd te blijven voldoen aan de toepasselijke wet- en regelgeving en aan artikel 14 GIBIT 2025. De daaruit voortvloeiende noodzakelijke maatregelen worden overeenkomstig de Overeenkomst en de GIBIT 2025 getroffen. Artikel 14 GIBIT 2025 blijft ongewijzigd van toepassing.
175	Art 14.8 GIBIT 2025	Inschrijver stelt voor om de bijstandsplicht nader in te kaderen door op te nemen dat inschrijver gehouden is om "redelijke medewerking" te verlenen. Kan Aanbestedende Dienst dit toevoegen?	Nee. De Aanbestedende dienst neemt de voorgestelde toevoeging niet over. Artikel 14.8 GIBIT 2025 bevat reeds de verplichtingen van Opdrachtnemer ten aanzien van de daarin bedoelde bijstand. De Aanbestedende dienst ziet geen aanleiding deze verplichting nader te beperken door toevoeging van het begrip "redelijke medewerking". Artikel 14.8 GIBIT 2025 blijft ongewijzigd van toepassing.
176	Art 32.5 GIBIT 2025	Deze bepaling bevat een RTO en RPO voor data. Inschrijver acht deze bepaling echter niet van toepassing omdat niet sprake is van een gewone SaaS-dienst waarbij de back-up verantwoordelijkheid bij leverancier ligt. Inschrijver stelt derhalve voor om dee bepaling buiten toepassing te verklaren. In het geval Aanbestedende Dienst van oordeel is dat deze bepaling wel degelijk van toepassing is, is het verzoek om dan toe te lichten op welke data en systemen deze bepaling van toepassing is.	Artikel 32.5 GIBIT 2025 is van toepassing voor zover het betrekking heeft op de door de opdrachtnemer geleverde ICT-prestatie. Het enkele feit dat Microsoft Sentinel in de gemeentelijke tenant staat, sluit toepassing op de door de opdrachtnemer beheerde of geleverde onderdelen niet uit. Voor Microsoft Sentinel en andere Microsoft-diensten die de gemeente zelf onder haar eigen contractrelatie afneemt en beheert, is de gemeente verantwoordelijk voor de back-up- en herstelafspraken met Microsoft. De opdrachtnemer is verantwoordelijk voor passende back-up- en herstelvoorzieningen voor de onderdelen die hij zelf levert of beheert, zoals een eventueel eigen SOC-portaal, eigen rapportage- of supportomgeving en door hem beheerde configuraties en documentatie. Ook blijft hij verantwoordelijk voor de continuïteit van zijn SOC-dienstverlening. Voor zover artikel 32.5 voor die opdrachtnemeronderdelen van toepassing is, geldt de hersteltermijn van 24 uur en de eis dat geen gegevens verloren mogen gaan, voor zover de opdrachtnemer die uitkomst binnen zijn beheer en zeggenschap kan waarborgen. De aanbestedingsstukken specificeren geen afzonderlijke RPO-waarde; die dient, waar nodig, per relevant onderdeel in het continuïteits- en herstelplan of DAP te worden uitgewerkt. De eis legt de opdrachtnemer geen garantie op voor herstel of nul gegevensverlies van gemeentelijke brondata of Microsoft-diensten buiten zijn feitelijke beheer en zeggenschap.

177	Art. 13.1 GIBIT 2025	De garantie in artikel 13.1 kan niet onbeperkt van aard zijn. Deze is immers ook in grote mate afhankelijk van de kwaliteit van data die van Aanbestedende Dienst wordt verkregen via de relevante koppelingen. Nauwkeurigheid is daarmee onhoudbaar als resultaatsverbintenis. Bovendien is deze bij de te leveren dienstverlening in feite al gekoppeld aan de Service Levels die partijen zullen afspreken in de SLA. Kan derhalve worden toegevoegd dat deze nauwkeurigheid wordt bepaald aan de hand van de nader overeen te komen Service Levels en dat het een inspanningsverbintenis betreft voor zover het gaat om factoren die van invleod kunnen zijn maar buiten de invloedssfeer van inschrijver liggen?	Nee. De Aanbestedende dienst neemt de voorgestelde toevoeging niet over. Artikel 13.1 GIBIT 2025 blijft ongewijzigd van toepassing. De daarin opgenomen verplichting wordt niet uitsluitend bepaald door de nader vast te stellen Service Levels en wordt niet generiek aangemerkt als een inspanningsverbintenis voor factoren buiten de invloedssfeer van Opdrachtnemer. Voor zover de werking of nauwkeurigheid van de betreffende toepassing aantoonbaar wordt beïnvloed door de kwaliteit, beschikbaarheid of volledigheid van gegevens of systemen waarvoor Opdrachtnemer niet verantwoordelijk is, wordt bij de beoordeling rekening gehouden met de concrete omstandigheden en de verantwoordelijkheidsverdeling zoals deze volgt uit de aanbestedingsstukken en GIBIT 2025. Artikel 13 GIBIT 2025 blijft ongewijzigd van toepassing.
178	Art. 13.2 GIBIT 2025	De aard van de dienstverlening kan met zich meebrengen dat specifieke treath intel informatie gedeeld moet worden met o.a. NCSC en andere partijen die lid zijn van het Cyclotronprogramma als onderdeel van het nationale programma om onze nationale cyberveiligheid te bevorderen . Deze intel kan niet gepseudo- of anonimiseerd worden, omdat het nu juist gaat om de intel zelf. Daarmee is het ook niet mogelijk om volledig uit te sluiten dat deze informatie tot Aanbestedende Dlenst te herleiden valt. Wel kan zij deze toezegging doen voor zover het persoonsgegevens betreft van Aanbestedende Dienst. Kan Aanbestedende Dienst bevestigen dat dit in het kader van deze bepaling voldoende is?	Het delen van dreigingsinformatie met derden valt niet onder artikel 13.2 GIBIT 2025, maar onder eis 2.27 van het Programma van Eisen. Daarin is bepaald dat verstrekking aan derden uitsluitend plaatsvindt na voorafgaande goedkeuring van Opdrachtgever. Aanbestedende Dienst staat toe dat Opdrachtnemer technische dreigingsinformatie, zoals Indicators of Compromise en aanvalstechnieken, deelt met het NCSC, de Informatiebeveiligingsdienst voor gemeenten (IBD) en vergelijkbare publieke samenwerkingsverbanden ter bevordering van de nationale cyberveiligheid. Daarbij gelden de volgende voorwaarden: er worden geen persoonsgegevens van of via Opdrachtgever gedeeld; informatie die herleidbaar is tot Opdrachtgever, zoals de naam van de organisatie of specifieke kenmerken van de omgeving, wordt alleen gedeeld na voorafgaande toestemming van Opdrachtgever per geval; het delen gebeurt via beveiligde kanalen en met inachtneming van gangbare classificatieafspraken (zoals TLP); de werkwijze wordt vastgelegd in het DAP.
179	Art. 13.3 GIBIT 2025	Inschrijver wijst erop dat Detectie-algoritmen in productie (ML-gebaseerde anomaly detection, behavioral analytics) vaak niet volledig explaineerbaar zijn op individueel niveau. Daarnaast kan Inschrijver niet toezeggen dat een specifieke detectiegebeurtenis volledig wordt geanalyseerd door middel van een forensische constructie zonder dat dit extra kosten geeft. Immers, dit is normaliter onderdeel van aanvullende Cert-dienstverlening die Aanbestedende Dienst in dat geval kan afnemen. Inschrijver stelt derhalve voor dat de individuele uitlegplicht beperkt is tot gevallen waarbij de algoritmische toepassing direct ten grondslag heeft gelegen aan een beslissing die de Opdrachtgever heeft genomen met rechtsgevolgen voor derden. Is dit akkoord voor Aanbestedende Dienst?	Nee. De gemeente vraagt geen forensische reconstructie van individuele detecties. CERT-dienstverlening staat als aanvullende, optionele component in het prijzenblad. De uitlegplicht betekent dat de opdrachtnemer per melding inzichtelijk maakt welke regel, welk model of welke signalen tot de melding hebben geleid, voor zover het gebruikte systeem dat mogelijk maakt. Volledige uitlegbaarheid van ML-modellen op individueel niveau wordt niet gevraagd.

180	Art. 17.3 en 17.4 GIBIT 2025	Inschrijver wijst erop dat het budget voor de aanbesteding relatief beperkt is en dat de totale aansprakelijkheid per jaar voor zaakschade en overige schade daarmee in disproportionele verhouding staat tot de jaarvergoeding. In dat kader wijst Inschrijver erop dat Aanbestedende Dienst op grond van de gids proportionaliteit ook is gehouden om rekening te houden met de risico's die de aanbestedende dienst daadwerkelijk loopt en de gebruikelijke aansprakelijkheidseis in de betreffende branche of voor de betreffende opdracht naar aard en omvang. In dat kader is van belang dat een gangbare aansprakelijkheidsbeperking in de IT-markt 1x ACV per contractjaar betreft, alsmede dat indirecte schade, gederfde winst en omzetverlies, vertragingsschade en gevolgschade volledig zijn aangesloten. In dat kader kan Inschrijver als middenweg Art. 17.4 GIBIT 2025 accepteren, maar stelt zij voor om het begrip zaakschade uit 17.3 te verwijderen (en deze bepaling dus enkel op persoonsschade te laten zien) en daarnaast om een aanvullende bepaling op te nemen waarmee indirecte schade, gevolgschade, gederfde winst en verlies van omzet, alsmede vertragingsschade volledig is uitgesloten. Kan Aanbestedende Dienst daarmee instemmen? Zo nee, waarom niet?	Nee. De Aanbestedende dienst neemt de voorgestelde wijzigingen niet over. Bij de beoordeling van de aansprakelijkheidsregeling is rekening gehouden met de aard, omvang en risico's van de onderhavige SIEM/SOC-dienstverlening. Artikel 17 GIBIT 2025 bevat reeds een gedifferentieerde en begrensde aansprakelijkheidsregeling, waarbij voor persoons- en zaakschade enerzijds en overige schade anderzijds afzonderlijke aansprakelijkheidsmaxima gelden. De Aanbestedende dienst acht deze regeling, mede gezien het kritische karakter van de dienstverlening en de mogelijke gevolgen van tekortkomingen op het gebied van informatiebeveiliging, continuïteit en incidentafhandeling, passend en proportioneel. De Aanbestedende dienst ziet daarom geen aanleiding zaakschade uit artikel 17.3 te verwijderen of aanvullende categorieën van indirecte of gevolgschade op voorhand geheel van vergoeding uit te sluiten. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
181	Art. 17.5 Gibit 2025	Inschrijver verzoekt Aanbestedende Dienst om te verduidelijken dat art. 17.5 sub iv (doorwerking van toezichthoudersboetes) uitsluitend van toepassing is als de boete opgelegd aan de Aanbestedende Dienst rechtstreeks verband houdt met een aantoonbare tekortkoming van Inschrijver, en niet geldt als de Aanbestedende Dienst door haar eigen handelen als verwerkingsverantwoordelijke een boete ontvangt waaraan Inschrijver geen of slechts deels verwijt treft. Voorts verzoekt inschrijver Aanbestedende Dienst om te bevestigen dat de aansprakelijkheidslimieten van art. 17.3 en 17.4 ook van toepassing zijn op schade die voortvloeit uit een beveiligingsincident waarbij Inschrijver als SOC-dienstverlener niet tijdig heeft gedetecteerd, zodat het commercieel risico voor inscrhijver proportioneel is ten opzichte van de overeengekomen vergoeding (dit betreffen immers situaties die onder de reguliere dienstverlening vallen en derhalve ook in aanmerking dienen te komen voor de aansprakelijkheidsbeperking, zodat inschrijver zich ook daartegen kan verzekeren.	Voor toepassing van artikel 17.5 sub iv GIBIT 2025 gelden de daarin opgenomen voorwaarden. Een aan de Aanbestedende dienst opgelegde toezichthoudersboete komt niet op grond van deze bepaling voor rekening van Opdrachtnemer voor zover deze uitsluitend voortvloeit uit handelen of nalaten van de Aanbestedende dienst en niet aan Opdrachtnemer kan worden toegerekend. Voor schade als gevolg van een beveiligingsincident, waaronder schade die verband houdt met het niet tijdig detecteren daarvan, geldt de aansprakelijkheidsregeling van artikel 17 GIBIT 2025. Of en in hoeverre de aansprakelijkheidsbegrenzingen van artikel 17.3 en 17.4 van toepassing zijn, wordt bepaald aan de hand van de aard en oorzaak van de betreffende schade en de in artikel 17 opgenomen uitzonderingen. De Aanbestedende dienst ziet geen aanleiding hiervoor een aanvullende of afwijkende aansprakelijkheidsregeling op te nemen. Artikel 17 GIBIT 2025 blijft ongewijzigd van toepassing.
182	Art. 19.3 GIBIT 2025	Inschrijver vindt een contractuele boete niet passend binnen de samenwerking die partijen beogen. Is Aanbestendende Dienst bereid deze buiten toepassing te verklaren?	Nee. De Aanbestedende dienst neemt het voorstel niet over. De in artikel 19 GIBIT 2025 opgenomen boetebepaling vormt onderdeel van de overeengekomen regeling rondom geheimhouding. De Aanbestedende dienst ziet, mede gelet op de aard van de SIEM/SOC-dienstverlening en de vertrouwelijkheid van de informatie die daarbij kan worden verwerkt, geen aanleiding deze bepaling buiten toepassing te verklaren. Artikel 19 GIBIT 2025 blijft ongewijzigd van toepassing.

183	Art. 20.2 GIBIT 2025	Inschrijver verzoekt Aanbestedende Dienst om te verduidelijken dat een cyberaanval op de eigen infrastructuur van inschrijver (bijv. een supply-chain-aanval op Inschrijver's SOC-platform) eveneens als overmacht kwalificeert. Kunt u dit bevestigen?	Een cyberaanval op de infrastructuur van de inschrijver, waaronder een supply-chain-aanval op diens SOC-platform, kwalificeert niet automatisch als overmacht. De beoordeling vindt per geval plaats aan de hand van artikel 20 GIBIT 2025 en de omstandigheden van het incident. Daarbij is onder meer relevant of de aanval en de gevolgen ondanks passende beveiligings-, continuïteits- en herstelmaatregelen redelijkerwijs niet konden worden voorkomen of beperkt. De opdrachtnemer blijft verantwoordelijk voor de overeengekomen beveiliging en continuïteit van de door hem beheerde onderdelen van de dienstverlening. Een aanval die samenhangt met onvoldoende passende maatregelen, of waarvan de gevolgen redelijkerwijs beperkt hadden kunnen worden, kan daarom niet zonder meer als overmacht worden aangemerkt. Het enkele feit dat een aanval van buitenaf komt, is niet voldoende om dat vast te stellen.
184	Art. 25 GIBIT 2025	Kan Aanbestedende Dienst verduidelijken op welke wijze Inschrijver een Software bill of materials moet aanleveren, op welk moment, en op welk deel van de ICT prestatie dit dan moet zien?	De SBOM ziet op de wezenlijke softwarecomponenten die onderdeel uitmaken van de geleverde ICT Prestatie. Dit omvat zowel eigen softwarecomponenten als relevante Derdenprogrammatuur. Voor Derdenprogrammatuur en andere door derden beheerde componenten verstrekt Opdrachtnemer de beschikbare SBOM- en keteninformatie en maakt hij eventuele beperkingen in de beschikbaarheid daarvan inzichtelijk.
185	Art. 28 GIBIT 2025	Inschrijver zou graag willen voorstellen de volgende nadere inkadering voor audits op te nemen: a) maximaal 1 audit per jaar, die b) tenminste 60 dagen van tevoren wordt aangekondigd, tenzij een toezichthouder een kortere termijn vereist, en c) dat auditors geheimhoudingsverplichtingen ondertekenen met Inschrijver die ten minste gelijkwaardig zijn aan art. 19 GIBIT, en (d) tot slot voor zover de audit daarop ziet dat deze uitsluitend plaatsvindt in een daarvoor bestemde testomgeving en niet in de productieomgeving van het SOC van Inschrijver, om verstoring van dienstverlening aan overige klanten te voorkomen. Kan Aanbestedende Dienst daarmee instemmen?	Nee. De Aanbestedende dienst neemt de voorgestelde nadere beperkingen niet over. Voor reguliere audits geldt het in het Programma van Eisen opgenomen maximum van twee audits per contractjaar. Wettelijke auditrechten en incidentele controles naar aanleiding van onder meer calamiteiten, beveiligingsincidenten, substantiële wijzigingen of compliancevraagstukken blijven hiervan uitgezonderd. De uitvoering van audits vindt plaats met inachtneming van artikel 28 GIBIT 2025 en wordt, voor zover de omstandigheden dit toelaten, vooraf afgestemd zodat de reguliere dienstverlening niet onnodig wordt verstoord. Daarbij wordt zorgvuldig omgegaan met vertrouwelijke informatie. De Aanbestedende dienst stemt niet in met een vaste aankondigingstermijn van 60 dagen of met een algemene beperking dat controles uitsluitend in een testomgeving mogen plaatsvinden. De aard, reikwijdte en wijze van uitvoering van een controle worden afgestemd op het doel en de omstandigheden van de betreffende audit. Het Programma van Eisen en artikel 28 GIBIT 2025 blijven ongewijzigd van toepassing.
186	Art. 10.11 GIBIT 2025	Inschrijver stelt voor om op te nemen dat van meerdere malen van overschrijding van hetzelfde Service Level als genoemd in dit artikel sprake is bij 3 achtereenvolgende overschrijdingen. Daarnaast stelt inschrijver voor om gezein de aard van de dienstverlening op te nemen dat artikel 10.11 uitsluitend ziet op incidenten die als p1 of p2 kwalificeren (en dus serieuze dreiging vormen). Kan Aanbestedende Dienst hiermee instemmen?	De opdrachtgever stemt niet in met het voorstel om “meerdere malen” uitsluitend te definiëren als drie achtereenvolgende overschrijdingen. Ook stemt de opdrachtgever niet in met het beperken van artikel 10.11 tot incidenten met prioriteit P1 of P2. De bepaling ziet op het herhaald niet behalen van hetzelfde overeengekomen Service Level. De escalatie- en verbeterplanprocedure uit PvE-eisen 8.8 tot en met 8.10 blijft daarnaast van toepassing.

187	Art. 4.3 GIBIT 2025	Inschrijver verzoekt Aanbestedende Dienst om te bevestigen dat de fatale termijn van art. 4.3 in de context van NIS2-implementatie (Cyberbeveiligingswet) en de AI Act uitsluitend geldt voor de specifieke onderdelen van de ICT Prestatie die rechtstreeks worden geraakt door de nieuwe wetgeving, en niet voor de gehele SOC/MDR-dienstverlening, alsmede dat Inschrijver recht heeft op redelijke aanpassingstermijn indien de bevoegde toezichthouder nadere guidance uitvaardigt. De Cyberbeveiligingswet (implementatie NIS2) en de AI Act bevatten verplichtingen die geleidelijk in werking treden en waarover toezichthouders (NCSC, Rijksinspectie Digitale Infrastructuur, AP) nog nadere invulling geven. Als de fatale termijn van art. 4.3 breed wordt uitgelegd, kan iedere wetswijziging op het snijvlak van cybersecurity en AI een automatische fatale deadline voor Inschrijver creëren, ook als de concrete verplichting door toezichthouders nog niet is geconcretiseerd. Inschrijver stelt voor om voor zover van belang na gunning te definiëren welke onderdelen van de ICT-prestatie mogelijk worden geraakt door veranderende wet- en regelgeving. Kunt u hiermee akkoord gaan?	De aanbestedende dienst stemt niet in met het voorstel om artikel 4.3 GIBIT 2025 in algemene zin te beperken tot vooraf benoemde onderdelen van de ICT-prestatie of om een algemene aanpassingstermijn te garanderen zodra een toezichthouder nadere guidance uitvaardigt.
188	Art. 7 GIBIT 2025	Kunt u bevestigen dat deze coördinatieverplichting en verantwoordelijkheid zich uitsluitend uitstrekt tot derde partijen die door Inschrijver zelf worden ingeschakeld bij de levering van de diensten?	Nee. Artikel 7 GIBIT 2025 is niet uitsluitend van toepassing op derde partijen die door Opdrachtnemer zelf worden ingeschakeld. Artikel 7 regelt juist de situatie waarin voor de uitvoering medewerking noodzakelijk is van derde partijen die geen hulppersoon van één van Partijen zijn. De verantwoordelijkheden ten aanzien van dergelijke derden worden bepaald overeenkomstig artikel 7 GIBIT 2025 en de in de aanbestedingsstukken vastgelegde verantwoordelijkheidsverdeling. De Aanbestedende dienst ziet geen aanleiding deze verplichtingen te beperken tot uitsluitend door Opdrachtnemer ingeschakelde derde partijen. Artikel 7 GIBIT 2025 blijft ongewijzigd van toepassing.
189	Bijlage I - Concept Model verwerkersovereenkomst, art. 3	Inschrijver stelt voor om ook een facturatieschema in de overeenkomst op te nemen op basis van de volgende kaders: 1) 50% van de implementatievergoeding direct na ondertekening van de definitieve overeenkomst; 2) 50% van de implementatievergoeding na Acceptie van de dienstverlening; 3) de periodieke vergoeding voor de diensten per jaar vooruit. Kan Aanbestedende Dienst instemmen met dit facturatieschema, en dit als zodanig ook opnemen in de conceptovereenkomst?	De Aanbestedende dienst stemt niet in met het voorgestelde facturatieschema. Wel wordt voor de implementatie en periodieke dienstverlening de volgende facturatiesystematiek gehanteerd: 30% van de eenmalige implementatievergoeding bij aanvang van de implementatie; de resterende 70% van de eenmalige implementatievergoeding na integrale Acceptatie; de periodieke vergoeding voor de dienstverlening wordt vanaf de start van de operationele dienstverlening per kwartaal vooruit gefactureerd. Voor Derdenprogrammatuur geldt artikel 11 GIBIT 2025. Voor het overige blijven de aanbestedingsstukken en GIBIT 2025 ongewijzigd van toepassing.

190	Bijlage A1, Eis TECH 13	Opdrachtgever stelt ISO/IEC 20000-certificering als minimumeis. De beoogde kwaliteit en beheersing van servicemanagement kan echter ook aantoonbaar worden geborgd door een professioneel ingericht Service Management System, ondersteund door relevante processen, rapportages, audits en andere certificeringen. Is opdrachtgever bereid de eis aan te passen, zodat een ISO/IEC 20000-certificering óf een aantoonbaar gelijkwaardig niveau van servicemanagement wordt geaccepteerd? Hiermee blijft het beoogde kwaliteitsniveau behouden, zonder de markt onnodig te beperken.	Op dinsdag 20 oktober 2026 jl. is middels een mededeling van aanbestedende dienst in een 1e Nota van Inlichtingen het volgende medegedeeld: 'De aanbestedende dienst deelt u hierbij mede dat in het document 'Bijlage A1 - Programma van Eisen – non functionals dd 08-10-2026' per abuis een uitvoeringseis is blijven staan die niet van toepassing is op deze aanbesteding. Het betreft de eis: "De Opdrachtnemer beschikt over een ISO20000 IT servicemanagement certificaat of vergelijkbaar. Indien vergelijkbaar toelichting op de procedures.' Deze eis vervalt!' Uw vraag is derhalve niet meer van toepassing.
191	Bijlage F1 Prijzenblad	Inschrijver constateert dat in het prijzenblad een afzonderlijke post voor CERT-dienstverlening en IR-retainers is opgenomen. Kan Opdrachtgever aangeven hoe CERT-ondersteuning momenteel is georganiseerd en welke onderdelen daarvan reeds zijn belegd? Tevens verzoekt Inschrijver te verduidelijken of van de toekomstige Opdrachtnemer wordt verwacht dat deze CERT-dienstverlening en incident response zelfstandig levert, aanvullend levert op bestaande voorzieningen, dan wel uitsluitend op afroep beschikbaar stelt.	Opdrachtgever beschikt op dit moment over een incident response-retainer bij een andere partij. Van Opdrachtnemer wordt niet verwacht dat hij zelfstandig CERT-dienstverlening of incident response levert als onderdeel van de reguliere dienstverlening. Bij incidenten die een respons vereisen die verder gaat dan de vooraf vastgelegde mandaten, schaalt Opdrachtgever in eerste instantie op met de partij op retainer. Opdrachtnemer ondersteunt en faciliteert die partij dan vanuit zijn informatiepositie (zie het antwoord op vraag 155). De post “CERT-dienstverlening en IR-retainers” in het Prijzenblad is een optionele prijscomponent zonder afnameverplichting. Deze telt niet mee in de beoordelingsprijs. Het onderdeel geeft Opdrachtgever inzicht in de mogelijkheid om deze dienstverlening in de toekomst, aanvullend of ter vervanging van de bestaande voorziening, op afroep bij Opdrachtnemer af te nemen. Inschrijver kan in de toelichting bij het Prijzenblad aangeven wat deze dienstverlening omvat en onder welke voorwaarden zij beschikbaar is.
192	Bijlage F1 Prijzenblad	Kan Aanbestedende Dienst verduidelijken welke onderdelen van het prijzenblad precies worden meegenomen in de prijsbeoordeling? Inschrijver begrijpt uit regel 40 dat uitsluitend de implementatiekosten en negen maal de jaarlijkse kosten onderdeel uitmaken van de beoordelingsprijs. Tegelijkertijd wordt bij de additionele dienstverlening vermeld dat het daar opgenomen fictieve volume wordt gebruikt voor beoordeling. Kan Aanbestedende Dienst bevestigen welke prijscomponenten wel en niet meetellen bij de vaststelling van de beoordelingsprijs?	De beoordelingsprijs bestaat uitsluitend uit de eenmalige kosten voor ontwerp en implementatie plus negen maal de jaarlijkse kosten voor de logbronnen (initiële scope), zoals weergegeven in regel 40 van het Prijzenblad. De onderdelen onder “Scope zonder afnameverplichting” en het uurtarief voor additionele dienstverlening tellen niet mee in de beoordelingsprijs. Deze onderdelen dienen om Aanbestedende Dienst inzicht te geven in de kosten van aanvullende dienstverlening. De vermelding bij de additionele dienstverlening dat het fictieve volume wordt gebruikt voor beoordeling, vervalt.
193	Bijlage F1 Prijzenblad	In het prijzenblad zijn voor de genoemde logbronnen de aantallen op 0 gesteld. Kunt u per logbron aangeven met welk indicatief of fictief aantal eenheden inschrijvers dienen te rekenen, zodat inschrijvingen op een uniforme en onderling vergelijkbare wijze kunnen worden opgesteld?	In het geactualiseerde Prijzenblad dat bij deze Nota van Inlichtingen wordt gepubliceerd, zijn per logbron de aantallen en de bijbehorende eenheid opgenomen. Inschrijvers rekenen met deze aantallen. De aantallen zijn indicatief en worden uitsluitend gebruikt voor de vergelijkbaarheid van de inschrijvingen. Er kunnen geen rechten aan worden ontleend. Bij wijzigingen in aantallen gedurende de looptijd gelden de aangeboden prijzen per eenheid. Deze zijn bindend (zie ook eis 5.5).
194	Bijlage F1 Prijzenblad	In het prijzenblad zijn voor de verschillende logbronnen geen aantallen ingevuld, terwijl de totaalprijs wordt gebruikt voor de beoordeling. Tevens moet de oplossing flexibel kunnen op- en afschalen bij wijzigingen in assets, gebruikers en logbronnen. Kunt u per logbron het huidige dan wel fictieve aantal eenheden verstrekken waarmee iedere inschrijver voor de prijsberekening dient te rekenen, zodat aanbiedingen onderling vergelijkbaar zijn?	In het geactualiseerde Prijzenblad dat bij deze Nota van Inlichtingen wordt gepubliceerd, zijn per logbron de aantallen en de bijbehorende eenheid opgenomen. Inschrijvers rekenen met deze aantallen. De aantallen zijn indicatief en worden uitsluitend gebruikt voor de vergelijkbaarheid van de inschrijvingen. Er kunnen geen rechten aan worden ontleend. Bij wijzigingen in aantallen gedurende de looptijd gelden de aangeboden prijzen per eenheid. Deze zijn bindend (zie ook eis 5.5).

195	Bijlage F1 Prijzenblad	In paragraaf 5.2 is opgenomen dat de uitwerking van de kwaliteitscriteria wordt beoordeeld met een rapportcijfer van 1 tot en met 10, waarbij vanaf een score hoger dan 6 fictieve meerwaarde wordt toegekend. Kunt u verduidelijken of iedere inschrijving individueel en absoluut wordt beoordeeld aan de hand van het beschreven beoordelingskader, of dat sprake is van een relatieve beoordeling waarbij de kwalitatief beste inschrijving per criterium automatisch het cijfer 10 en daarmee de maximale fictieve meerwaarde ontvangt? Kunt u tevens bevestigen of het mogelijk is dat geen enkele inschrijver een 10 behaalt, dan wel meerdere inschrijvers hetzelfde cijfer behalen?	De Aanbestedende dienst bevestigt dat sprake is van een absolute en individuele beoordeling. Iedere Inschrijving wordt per kwaliteitscriterium afzonderlijk beoordeeld aan de hand van het in de aanbestedingsstukken opgenomen beoordelingskader en de daarbij behorende cijferschaal. Er is geen sprake van een relatieve beoordeling waarbij de kwalitatief beste Inschrijving automatisch het cijfer 10 ontvangt. Een cijfer 10 wordt uitsluitend toegekend indien de betreffende uitwerking naar het oordeel van de aanbestedende dienst voldoet aan de voor dat cijfer beschreven beoordelingsmaatstaf. Het is derhalve mogelijk dat geen enkele Inschrijver een 10 behaalt. Eveneens is het mogelijk dat meerdere Inschrijvers voor een kwaliteitscriterium hetzelfde cijfer behalen. De gunnings- en beoordelingssystematiek blijft ongewijzigd van toepassing.
196	Bijlage F1 Prijzenblad	Kan Opdrachtgever een afzonderlijke prijscomponent opnemen onder "Diensten zonder afnameverplichting" voor het aansluiten van een nieuwe logbron waarvoor geen standaard Microsoft Sentinel connector beschikbaar is? Zonder een dergelijke prijsregel kunnen Inschrijvers verschillende aannames hanteren ten aanzien van ontwikkel-, implementatie- en beheerkosten, hetgeen de onderlinge vergelijkbaarheid van inschrijvingen kan beïnvloeden.	Aanbestedende Dienst neemt dit verzoek niet over. De aard en omvang van het aansluiten van een niet-gespecificeerde logbron zonder standaardconnector kan sterk verschillen. Dit laat zich niet op een zinvolle manier in één prijsregel vangen. Voor de in eis 2.2 genoemde logbronnen geldt eis 2.13 en zijn de kosten inbegrepen in de aangeboden prijzen. Het aansluiten van aanvullende, niet in de aanbestedingsstukken genoemde logbronnen wordt gedurende de looptijd behandeld als meerwerk conform eis 5.10. Opdrachtnemer doet hiervoor vooraf een voorstel, op basis van het in het Prijzenblad opgenomen uurtarief voor additionele dienstverlening.
197	Bijlage F1 Prijzenblad	Ten aanzien van de onderdelen opgenomen onder "Scope zonder afnameverplichting" in het prijzenblad verzoekt Inschrijver te verduidelijken of van iedere Inschrijver wordt verwacht dat hij alle genoemde optionele diensten kan leveren. Indien een Inschrijver een of meer van deze diensten niet aanbiedt of niet kan leveren, verzoekt Inschrijver aan te geven welke gevolgen dit heeft voor de beoordeling van de inschrijving, de puntentoekenning en/of de geldigheid van de inschrijving.	Inschrijver is niet verplicht de onderdelen onder “Scope zonder afnameverplichting” aan te bieden. Biedt Inschrijver een onderdeel niet aan, dan vermeldt hij in het Prijzenblad “niet van toepassing”. Dit heeft geen gevolgen voor de geldigheid van de inschrijving of voor de beoordeling, omdat deze onderdelen niet meetellen in de beoordelingsprijs (zie het antwoord op vraag 192). Eis 5.2 wordt in die zin verduidelijkt. De in het Programma van Eisen beschreven dienstverlening, waaronder 24/7 detectie, triage, analyse en escalatie conform eis 2.20, maakt onverkort deel uit van de basisdienstverlening en moet zijn inbegrepen in de beoordelingsprijs.
198	Bijlage A1, Eis TECH25	Aanbestedende Dienst vraagt om aan App. Kan Aanbestedende Dienst bevestigen dat een via SmartPhone bereikbare en bruikbare webapplicatie voldoende om deze eis in te vullen?	TECH25 komt te vervallen, zie vraag 37.
199	Bijlage A1, Eis SLA8	Ten aanzien van eis SLA8 merkt Inschrijver op dat een deel van de definitie van "Detectietijd" buiten de invloedsfeer van Opdrachtnemer ligt. Het moment waarop een beveiligingsincident daadwerkelijk ontstaat is niet altijd objectief vast te stellen en kan bovendien voorafgaan aan de beschikbaarheid van relevante logging, telemetrie of detectiesignalen. Kan Aanbestedende Dienst akkoord gaan met de volgende aangepaste definitie van detectietijd: "De tijd tussen het moment waarop een beveiligingsincident binnenkomt in het SIEM-platform en het moment waarop het incident door het SOC wordt gedetecteerd en geclassificeerd." Indien Aanbestedende Dienst hiermee niet akkoord gaat, verzoekt Inschrijver toe te lichten op welke wijze het moment van ontstaan van een beveiligingsincident objectief, reproduceerbaar en voor alle partijen verifieerbaar wordt vastgesteld.	De opdrachtgever verwijst naar het antwoord op vraag 25 in deze Nota van Inlichtingen.

200	Bijlage A1, Eis SLA26	Inschrijver constateert dat de SLA voorziet in een boeteregeling waarbij reeds vanaf twee overschrijdingen per maand een boete kan worden opgelegd tot maximaal 100% van de maandelijkse vergoeding. Inschrijver is van mening dat dergelijke boetes onvoldoende aansluiten bij het karakter van cybersecurity-dienstverlening, waarbij continue verbetering, transparantie en samenwerking centraal staan. Is Aanbestedende Dienst bereid de boeteregeling te vervangen door een systeem van een verplicht verbeterplan, zodat eventuele tekortkomingen primair leiden tot herstel- en verbetermaatregelen in plaats van een punitieve sanctie?	De opdrachtgever is niet bereid SLA26 te verwijderen of de boeteregeling te vervangen door uitsluitend een verplicht verbeterplan. De boeteregeling blijft naast de escalatie- en verbeterplanprocedure van eisen 8.8 tot en met 8.10 van toepassing. Zoals eerder verduidelijkt, wordt SLA26 niet toegepast op het aantal beveiligingsincidenten. De grondslag is twee of meer aantoonbare, aan de opdrachtnemer toerekenbare overschrijdingen van de toepasselijke servicenorm per prioriteitscategorie in een kalendermaand. Niet-toerekenbare overschrijdingen tellen niet mee. De in SLA26 genoemde boetepercentages blijven gelden.
201	Bijlage A, Eis 2.2	Inschrijver is van mening dat niet alle genoemde logbronnen relevant zijn voor de uitgevraagde security monitoring. Gaat opdrachtgever ermee akkoord dat Inschrijver logbronnen risico-gebaseerd aansluit waaronder in elk geval die logbronnen die input leveren voor de in eis 2.1 genoemde use-cases? Zo voorkomen we dat niet-relevante logbronnen worden aangesloten wat onnodig hoge kosten voor gemeente Vijfheerenlanden met zich mee brengt, en handelen we in lijn met PvE-eis 2.22.	Nee, we stemmen hier niet mee in.
202	Bijlage A, Eis 4.19	Inschrijver maakt voor de uitvoering van SIEM/SOC-dienstverlening gebruik van een eigen Microsoft Sentinel-omgeving, waarin detectieregels, use-cases, analytics rules en automatiseringen centraal worden beheerd voor meerdere klanten. Via Microsoft Lighthouse wordt de klantspecifieke Sentinel -instance binnen deze omgeving gekoppeld aan de Microsoft Sentinel-omgeving van Opdrachtgever voor monitoring en beheer. Bij deze werkwijze blijft alle log- en detectiedata eigendom van en opgeslagen binnen de tenant van Opdrachtgever, terwijl Inschrijver de dienstverlening centraal kan beheren en doorontwikkelen. Dit draagt tevens bij aan veiligheid, overdraagbaarheid en voorkomt afhankelijkheid van één leverancier. Kan Opdrachtgever bevestigen dat deze wijze van dienstverlening binnen de uitgangspunten van de aanbesteding is toegestaan? Indien dit niet het geval is, verzoeken wij u toe te lichten waarom dit niet mogelijk is.	Ja, deze wijze van dienstverlening is toegestaan, mits Microsoft Sentinel in de Microsoft-tenant van de opdrachtgever blijft ingericht als de primaire Sentinel-omgeving en de gemeente daarover de technische en administratieve zeggenschap behoudt, conform eis 2.16.
203	Bijlage A, Eis 4.19	Inschrijver ondersteunt de gevraagde SIEM-dienstverlening met Microsoft Sentinel conform de uitgangspunten van de aanbesteding. Voor automatisering, orkestratie, verrijking, responsacties en incidentafhandeling kan gebruik worden gemaakt van een geïntegreerd SOAR-platform dat informatie uitwisselt met Microsoft Sentinel en andere relevante securitybronnen. Kan Opdrachtgever bevestigen dat een dergelijke architectuur is toegestaan, mits Microsoft Sentinel het centrale SIEM-platform binnen de omgeving van Opdrachtgever blijft	Ja. Een geïntegreerd SOAR-platform mag worden ingezet voor automatisering, orkestratie, verrijking, responsacties en incidentafhandeling, mits Microsoft Sentinel binnen de Microsoft-tenant van de opdrachtgever het centrale platform blijft voor beveiligingsmonitoring, correlatie, onderzoek en incidentregistratie, zoals vereist in eis 4.19. Het aanvullende platform mag de toegang, zeggenschap, beveiliging, prestaties, overdraagbaarheid of gegevensbescherming van de opdrachtgever niet beperken. Relevante gegevens en klantspecifieke configuraties moeten rechtstreeks toegankelijk blijven voor de opdrachtgever. Responsacties in de gemeentelijke omgeving mogen uitsluitend plaatsvinden binnen vooraf schriftelijk vastgelegde bevoegdheden en mandaten.

204	Bijlage A, Eis 5.1	Inschrijver constateert dat het huidige prijzenblad beperkt ruimte biedt voor prijsmodellen waarin de dienstverlening bestaat uit een combinatie van vaste periodieke kosten en variabele componenten die niet rechtstreeks afhankelijk zijn van het aantal of type aangesloten logbronnen. Kan Opdrachtgever het prijzenblad uitbreiden met de volgende prijscomponenten, zowel voor de dienstverlening binnen scope als voor de diensten zonder afnameverplichting: - Vaste periodieke kosten voor de SIEM/SOC-dienstverlening; - Variabele periodieke kosten voor de SIEM/SOC-dienstverlening op basis van maximaal drie afzonderlijke eenheden, waarvan de prijsstelling niet of slechts indirect afhankelijk is van het aantal of type aangesloten logbronnen.	Aanbestedende Dienst neemt dit verzoek gedeeltelijk over. In het geactualiseerde Prijzenblad wordt binnen de initiële scope een regel “Vaste periodieke kosten SIEM/SOC-dienstverlening (per jaar)” toegevoegd. Deze kosten tellen mee in de beoordelingsprijs (negen maal de jaarlijkse kosten). Voor variabele periodieke kosten die niet direct afhankelijk zijn van het aantal of type logbronnen kan Inschrijver gebruikmaken van de regels “per jaar/asset” en “overig, namelijk”. Hij vermeldt daarbij de gehanteerde eenheid. Aanbestedende Dienst heeft in het geactualiseerde Prijzenblad indicatieve aantallen opgenomen voor de eenheden gebruikers, endpoints en servers (zie het antwoord op vraag 193). Uitsluitend componenten die op deze eenheden zijn gebaseerd, tellen mee in de beoordelingsprijs. Hanteert Inschrijver een andere eenheid, dan wordt die component niet beoordeeld. Inschrijver blijft dan wel gebonden aan het opgegeven tarief. De kosten mogen niet dubbel worden opgenomen. Kosten die in de vaste periodieke kosten zijn verwerkt, worden niet ook per logbron in rekening gebracht, en omgekeerd. Het Prijzenblad wordt aangepast. Overige aanbestedingsstukken wijzigen niet.
205	Bijlage A, Eis 5.5	Hoe kan Inschrijver op het Prijzenblad de hier gevraagde gegevens invullen? Op dit moment kunnen alleen de gele velden worden ingevuld, maar die dienen een ander doel.	Het prijsblad is bijgewerkt om betere represenatie van de feiten te faciliteren.
206	Bijlage A, Eis 5.5	Opdrachtgever geeft in eis 5.5 aan om uitgangspunten en aannames mbt de prijscomponenten te vermelden en toe te lichten. Inschrijver stelt voor om een kostentoelichting (ICT prestatie beschrijving) te kunnen bijsluiten waarin genoemde punten worden beschreven en tevens een prijsonderbouwing wordt verstrekt van de ingevulde prijzen in het prijzenblad. In dit overzicht kan tevens worden toegelicht waarom bij sommige posten een nul-waarde of "nvt" is ingevuld. Is dit akkoord?	Ja, dit is akkoord. Inschrijver mag bij het Prijzenblad een afzonderlijke kostentoelichting voegen. Daarin beschrijft hij de gehanteerde eenheden, tarieven, uitgangspunten en aannames zoals bedoeld in eis 5.5. Daarnaast kan hij in deze toelichting aangeven waarom bij bepaalde posten € 0,00 of “niet van toepassing” is ingevuld. Daarbij geldt het volgende: Het Prijzenblad is leidend. Bij strijdigheid tussen de kostentoelichting en het Prijzenblad prevaleert het Prijzenblad. De kostentoelichting mag geen aanvullende prijzen of kostenposten bevatten die niet in het Prijzenblad zijn opgenomen (zie ook eis 5.9). De kostentoelichting mag geen voorbehouden of voorwaarden bevatten. Een inschrijving met voorbehouden of voorwaarden is ongeldig (§ 4.2.2 Aanbestedingsdocument). De kostentoelichting wordt niet beoordeeld in het kader van de gunningscriteria en telt niet mee voor het maximale aantal pagina’s van subgunningscriteria A, B en C.
207	Bijlage A, Eis 5.5	Kan Aanbestedende Dienst bevestigen dat het tussen partijen overeengekomen SLA en Exit plan in prioriteit prevaleert direct na de Overeenkomst? Zo ja, Kan Aanbestedende Dienst deze in rangorde opnemen als opgenomen in dit artikel?	Nee. Zie tevens het antwoord op vraag 65. De SLA en het Exitplan vormen een nadere uitwerking binnen de kaders van de aanbestedingsstukken, de Inschrijving en de Overeenkomst en krijgen geen zelfstandige hogere positie in de rangorde van artikel 1.3.
208	Bijlage A, Tabel 9.2	Kan Aanbestedende Dienst bevestigen dat tabel 9.2 een richtinggevend uitgangspunt vormt voor de op grond van eis 8.22 gezamenlijk op te stellen RACI-matrix en niet bedoeld is als een voorgeschreven, ongewijzigde verantwoordelijkheidsverdeling? Indien dit niet het geval is, verzoekt Inschrijver aan te geven welke onderdelen van tabel 9.2 als bindende eis moeten worden beschouwd.	Ja. Tabel 9.2 dient te worden beschouwd als een richtinggevend uitgangspunt voor de op grond van eis 8.22 gezamenlijk op te stellen RACI-matrix. De tabel is niet bedoeld als een onverkort voorgeschreven verantwoordelijkheidsverdeling. De definitieve RACI-matrix wordt na gunning in gezamenlijk overleg tussen Opdrachtgever en Opdrachtnemer opgesteld en vastgesteld, met inachtneming van de in het Programma van Eisen beschreven rollen, taken en verantwoordelijkheden. Nadere invulling en detaillering van de verantwoordelijkheidsverdeling is daarbij toegestaan, mits deze in lijn blijft met de doelstellingen en uitgangspunten van het Programma van Eisen.

BIJLAGEN: Bijlage 1 bij deze NvI - Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 30-10-2026.xlx